View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by AIS Electronic Library (AISeL)

Privacy fatigue: The effect of privacy control complexity on consumer electronic information disclosure

Completed Research Paper

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

Courtenay M. Evans
Brigham Young University
Provo, UT, USA
court10a@gmail.com

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

Jeffry S. Babb
West Texas A&M University
Canyon, TX, USA
jbabb@wtamu.edu

Abstract

When online social networks change privacy control features (i.e. methods of sharing consumer information), the result is often media attention and public outcry. Facebook introduced new privacy controls in 2009 causing the Electronic Frontier Foundation to accuse them of pushing users to disclose more information than ever before. However, there is little research to indicate that such practices are effective. Although research on privacy control designs is emerging, few studies adopt theoretical bases or empirically test the results of the design. This study fills a theoretical and methodological gap in the context of privacy controls. We adopt feature fatigue theory from the marketing literature to explain the effects of privacy control complexity on consumer self-disclosure behavior. We test our model with a unique longitudinal field experiment wherein participants are randomly assigned to various treatments of privacy control complexity. We found support for our theoretical extension we term "privacy fatigue."

Keywords: privacy fatigue, information privacy, privacy controls, information disclosure, feature fatigue, field experiment

Privacy fatigue: The effect of privacy control complexity on consumer electronic information disclosure

Completed Research Paper

Introduction

As consumers disclose an increasing amount of information to online sources, the issue of privacy and user privacy controls (a.k.a. *privacy settings*) has grown. When Online Social Networks (OSN) like Facebook, for example, change privacy control features and methods of sharing user information, the result is often media attention and public outcry (Hoadley et al. 2010). In particular, researchers and other privacy-conscious writers have expressed concern over whether companies such as Facebook intentionally construct their privacy controls to entice users to disclose and share more information. When Facebook introduced new privacy settings in 2009, the Electronic Frontier Foundation (EFF) accused the social media site of pushing users to disclose more information to the public than ever before (Bankston 2009). However, little research indicates that such practices are effective, as it is also unclear as to what end such changes are undertaken.

In this context, both a theoretical and methodological gap exists that should be filled. Whereas theories exist that can help explain consumers' intentions to disclose information online (Dinev and Hart 2006; Keith et al. 2013; Posey et al. 2010), how consumers' perceived control over information affects disclosure (Brandimarte et al. 2013), and how privacy concerns are formed (Lowry et al. 2011; Xu et al. 2012b), theory in information systems (IS) research that explains the consequences of privacy control design on consumer information disclosure is in short supply. This is not to say that privacy setting design has not been researched. Rather, there is little theory regarding the relationship between information disclosure behaviors and privacy setting design. We thus adapt a theory from the marketing literature called *feature fatigue* that is used to explain the longitudinal effects of product features on consumer satisfaction and product usage (Thompson et al. 2005). Termed here as *privacy fatigue*, our related concept refers to the tendency of consumers to disclose greater information over time when using more complex and less-usable privacy controls.

The methodological gap addressed by this study concerns the combination of data collected about actual consumer information disclosure over time with experimental manipulation. Although Stutzman et al. (2013) and other studies have captured user information disclosure over time, we combine actual consumer data with experimentation. To understand the effects of privacy fatigue, researchers must collect real longitudinal behaviors while also employing experimental treatments to establish causality. No study of our knowledge has done this. Therefore, we employ a unique field experiment research design based on a mobile app and accompanying website application developed specifically for this research. Our sample consisted of 441 current mobile smartphone users who used the app over a three-month period.

Our results demonstrate the varying effects of privacy control capabilities versus ease-of-use. In particular, we found that expected privacy control utility was based primarily on the perceived capabilities of the privacy controls whereas long-term privacy control settings were based primarily on perceived ease-of-use. The implication of this finding is that consumer software vendors can create complex controls that both excite consumers initially yet also encourage excessive information disclosure over time because of the inherent tradeoff in usability.

The following section outlines the background literature on consumer information privacy controls. The next section describes the privacy fatigue theory. After that, we explain the methodology in detail and review the analysis of the results. The final section outlines specific implications for research and practice.

Background Literature on Privacy Controls

Applicable research on privacy controls is growing fast and methodologies are improving[1]. Early studies of privacy controls were typically based on laboratory studies and behavioral intentions or reported (unverified) behaviors. For example, some studies surveyed users for their intentions or beliefs and a report of existing privacy settings. Hargittai (2010) conducted a longitudinal survey of a group of students regarding Facebook usage, experience with changing privacy settings, and stated number of times the user changed privacy settings, finding that online skills increased the number of times people stated that they changed their privacy settings. Most other survey studies were cross-sectional and surveyed participants for stated privacy control behaviors and user beliefs (Ayalon and Toch 2013; Ibrahim et al. 2012; Joinson 2008; Walrave et al. 2012). In general, these studies analyzed the effects of information timeliness, privacy strategies, sense of control, demographics, gratification, and privacy concerns about stated privacy settings and reported disclosure. Although these studies helped move understanding of privacy controls forward, it is well-documented that privacy intentions are relatively poor predictors of *actual* information disclosure (Acquisti and Grossklags 2004)—in the form of personal information disclosure and the accompanying privacy settings (Keith et al. 2013).

Because these studies request stated privacy control behaviors, they cannot guarantee that their participants reported their true privacy settings. Recent reviews of privacy research calls for empirical studies about how privacy concerns affect actual outcomes (Belanger and Crossler 2011; Smith et al. 2011). Accordingly, other studies have developed unique tools and methodologies for capturing actual consumer privacy settings. Perhaps the most common method for assessing privacy controls has been Web-scraping actual user profiles from OSNs. Although some of these studies scraped for information multiple times (Acquisti and Gross 2006; Dey et al. 2012; Lewis et al. 2008; Williams et al. 2011), the majority of these studies scraped for information only once (Gross and Acquisti 2005; Guo and Chen 2012; Liu et al. 2011; Madejski et al. 2012; Meeder et al. 2010; Netter et al. 2013). In general, these studies found that users become more oriented toward privacy over time and that significant discrepancies exist between both users' intended and reported privacy settings and the user's actual privacy settings. One study went further and found that users with more private friends, high application use, and a preference for popular music tend to use stricter privacy settings (Lewis et al. 2008). Additionally, we found only one study that incorporates survey data regarding participants' privacy attitudes, concerns, and awareness of privacy controls in particular (Acquisti and Gross 2006). Although these studies improved the measurement of disclosure intentions and self-reported behaviors, Web-scraping does not allow for experimentation and random assignment to treatment conditions.

Other studies have sought to explain causal effects of privacy control design. Benisch et al. (2011) and Sadeh (2009) examined location-based privacy controls of users in combinations of laboratory and field experiment settings. Benisch et al. (2011) and Sadeh (2009) studied user addition of privacy policies in regards to sharing user locations, including time of day sensitivity, by creating applications and either running simulations with these applications or requiring users to use them over a period of time. In studying the creation of location-sharing policies over time, these studies suggested that more granular privacy settings encourage more user information sharing and that users tend to relax settings over time. These studies are helpful in taking steps forward in the design of privacy settings by recognizing that users require a certain level of granularity. However, all users were allowed the same privacy controls; while they could update and create policies unique to their situations, the user interface for the privacy controls was identical. Our study extends the concept of privacy setting granularity by allowing for experimental manipulation of different kinds of privacy controls, ranging from simple to complex.

As noted, few studies have examined privacy control settings over time and in an experimental setting. Clearly, consumers may decide to change their privacy settings over time. For example, a researcher may choose to examine initial information disclosure behavior using a unique research tool like a mobile app with the intention of carefully monitoring both the information disclosed as well as the privacy settings chosen. A participant might initially leave the default settings "as is" because of time constraints, yet plan to adjust them later if given the chance. As a result, such participants might omit entering personal

[1] The following literature review includes studies only on privacy *controls* or *settings* and not actual information disclosure alone.

information because they have not adjusted their privacy settings. A researcher may mistakenly interpret this consumer behavior as representing those who are highly concerned about privacy risks. Yet, in reality, such participants are simply trying to rush to complete the experimental task (e.g., to earn the extra credit as quickly as possible). The solution to this problem is to implement a longitudinal research design in which the participants are free to adjust their privacy settings over time without artificial constraints. Although some studies have scraped longitudinal data from existing OSN, this method does not allow for experimental manipulations that are required to establish causality.

The experiments conducted by Brandimarte et al. (2013), whereas not explicitly focusing on privacy controls or settings, resulted in important implications for privacy setting research. This research found that people who felt in control of their information were more likely to disclose information, suggesting that those with more granular privacy setting controls would disclose more information than those without these controls. Our research seeks also to determine differences between user disclosure behaviors with different granularity options; however, we seek to study how these behaviors change over time in according to user perceptions of the ease-of-use and complexity of privacy settings (and thus control over their information). By adjusting actual privacy settings and measuring actual disclosure in an OSN setting, we can gain further insight into the effects of privacy control granularity.

Theory and Hypotheses Based on Privacy Fatigue

The theoretical lenses used in recent electronic information privacy research vary somewhat (for a review, see Li 2012) but are primarily dominated by social exchange theory (e.g. Posey et al. 2010), privacy calculus theory (e.g. Keith et al. 2010; Keith et al. 2013; Keith et al. 2012; Xu et al. 2010), and various control theories (e.g. Hoadley et al. 2010; Xu et al. 2012b). Privacy calculus establishes the tradeoff between benefits and risks in general electronic information disclosure (Dinev and Hart 2006). Social exchange theory better explains the consumer's information tradeoff with other social network consumers based on the desire for reciprocity (Emerson 1976). Theories on control help to explain the consumers desire for control (Bandura 2001) over personal information and the illusion that the consumer has control over their personal information (Langer 1975). Although each theory has been useful in explaining some degree of consumer disclosure intentions and privacy concerns, they do not help to explain the specific effects of the privacy control design characteristics that influence actual behaviors. We leverage new theoretical insights from the marketing literature to make this connection.

Leveraging Feature Fatigue Theory in a Privacy Control Context

From the marketing literature, *feature fatigue* theory describes the longitudinal effect of a product's number of features, capability and usability on consumer satisfaction, taking into account user expertise (Thompson et al. 2005). Although "usability" is the construct named by Thompson et al. (2005), in HCI literature, usability is more a broadly defined, complex and multidimensional construct (Brooke 1996; Calero et al. 2005; Hornbæk 2006; Nielsen 1994). However, for theoretical succinctness of our model, we narrow "usability" to ease-of-use to match the intended definition in Thompson et al. (2005). Thompson et al. (2005) found that consumers initially rate products with many features as highly capable and are very satisfied with this product. However, once the consumer has used the product for several months, they become disillusioned and exhausted by the number of product features, and satisfaction drops. Consumers that used products with fewer features and were initially less satisfied. However, they found the product to be much more usable in the long term and are satisfied with this product. Figure 1 overviews feature fatigue theory.

Feature fatigue is based on two core theories. First, economic utility theory is used to explain the additive utility increase for all product features (Lancaster 1971). Consequently, more features make a product more appealing. Each feature is seen as a value-add to the product, and therefore, increases consumers' perceptions of product capability. Consequently, companies continually add features to lines of consumer products to satisfy the insatiable need of consumers to find products appealing.

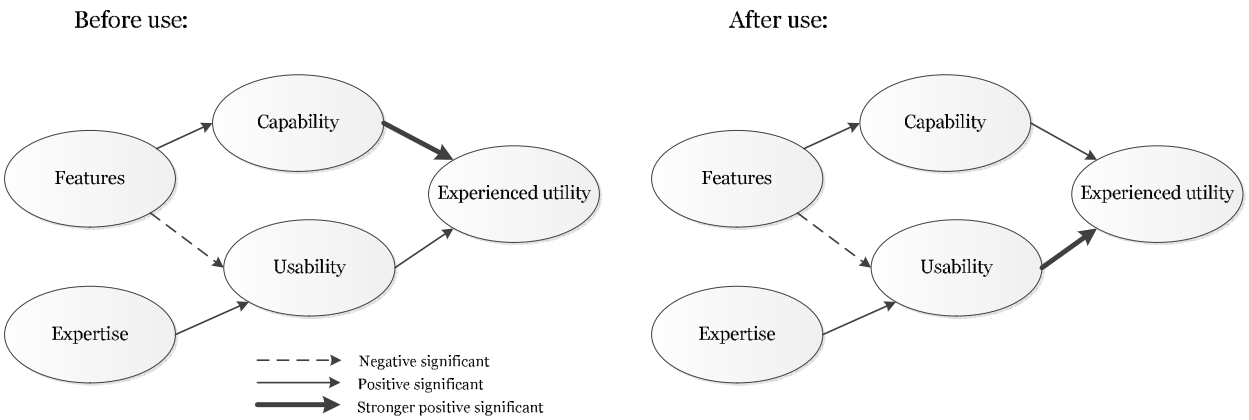


Figure 1. Feature Fatigue Model Adapted from (Thompson et al. 2005)

Second, feature fatigue draws from the theoretical proposition that product complexity also causes stress and anxiety (Mick and Fournier 1998). Whereas perceived product capability increases with the number of features, perceived product ease-of-use may be negatively affected by the number of features (Wiklund 1994)—causing a conundrum with consumers. Consumers may struggle with more complex products due to the high number of features and deem the product unusable. For example, consumers evaluated products negatively when the products were described as manually operated and positively when described as fully automatic, showing that ease-of-use and learning costs are taken into account when consumers consider various product features (Mukherjee and Hoyer 2001). Finally, feature fatigue takes expertise into account when considering ease-of-use, because experts are more successful using technologies, such as mobile devices, than novices (Ziefle 2002).

These two theories combined illustrate the paradox between product capability and ease-of-use; consumers evaluate products on not only functionality (i.e., product capability) but also ease-of-use (i.e., product ease-of-use). Features can have a positive effect on consumers' perceived capability and a negative effect on consumers' perceived ease-of-use of a product. By itself, the capability/ease-of-use tradeoff is not new or particularly interesting. However, Thompson et al. (2005) hypothesized and demonstrated across a variety of products that the effects of feature capability and ease-of-use reverse in importance over time. The reversal that takes place between perceived capability and ease-of-use and the product's utility is not that one relationship is positive and the other is negative and then this switches. Rather, the reversal is that capability has a greater positive weight than ease-of-use before usage, then ease-of-use has a greater positive weight than capability after usage (see Figure 1); the strength of the relationships is reversed.

The Effects of Adding Features: From Feature Fatigue to Privacy Fatigue

We extend and apply this theoretical foundation into the realm of privacy controls. Feature fatigue is based on the assumption that products have features that are perceived as value-added by consumers. As with physical products, digital products also have features with varying capability and ease-of-use.

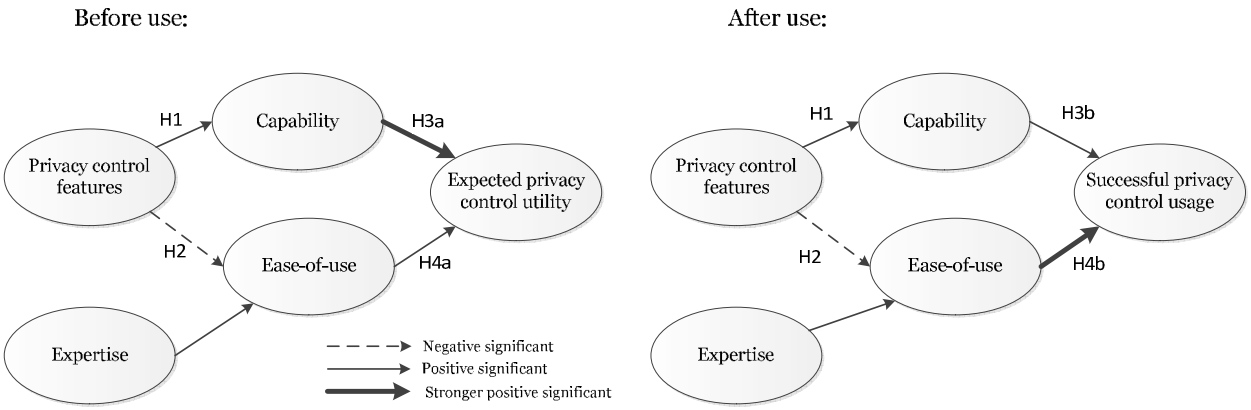


Figure 2. Privacy Fatigue Model

Feature fatigue theory, while explicitly analyzing physical technology products, can and should be applied to the digital sphere to include products such as mobile applications and website services. Privacy controls are a feature of any digital product that allows consumers to share personal information amongst each other. Privacy controls vary greatly in practice from very simple or coarse to more complex and granular. By feature or control complexity and granularity, we refer to the number of options a user has in managing their privacy settings. As additional privacy control features are added, consumers have a greater ability to differentiate information sharing among various types of social network relationships and information types. Research has demonstrated that both information privacy and information sharing are, indeed, a value-added commodity that is desirable to consumers (Choi and Choi 2007; Hui et al. 2007; Mai et al. 2010; Stone et al. 1983). Privacy controls, in particular, play an important role in adjusting the privacy risk versus benefit tradeoff in the consumer's favor (Debatin et al. 2009). Therefore, we hypothesize:

> *H1: As the level of privacy control features that are perceived as beneficial to consumers increases, the consumers' perceived capability of the privacy controls increases.*

In addition, feature fatigue assumes that—at some point—each additional product feature reduces the perceived ease-of-use of the overall product and that ease-of-use is also desirable to consumers (Thompson et al. 2005). The reduction in perceived ease-of-use must cause a real cost to the consumer. This may be in the form of cost from initially learning to use the product, or a time cost from the increased complexity of performing the intended product functions.

The usability-cost assumption will likely also hold true in the privacy control context. In Thompson et al.'s (2005) experiment, DVD player consumers were examined. Consumers were monitored at an electronics store. Those who purchased a "simple" DVD player would have had only the seven most basic features such as "Play," "Stop," "Pause," and "Skip." They were surveyed and compared to consumers who purchased DVD players with a more complex set of features. However, additional DVD player features only serve purpose to increase the granularity of the original seven features. For example, "skip forward" is modularized into skipping by chunks, skipping continuously at variable speeds, or skip to the end. Similarly, "Play" can be decomposed into playing at a normal speed, 2x speed, ½ speed, and so on.

The DVD player modularization is similar to the increased granularity of features common among privacy controls. Privacy controls may offer simple global setting such as "Share information with everyone/friends only/nobody" for all types of information. This is very similar to the current features offered by the Twitter™ social network. Conversely, privacy controls may also be much more granular and complex if they differentiate among types of friends and types of information such as those offered by Facebook™. In this case, the total number of privacy control options that need to be considered when deciding on a consumer's overall privacy profile is equal the number of levels of information types multiplied by the number of groups or types of social network relationships (see Figure 3 example).

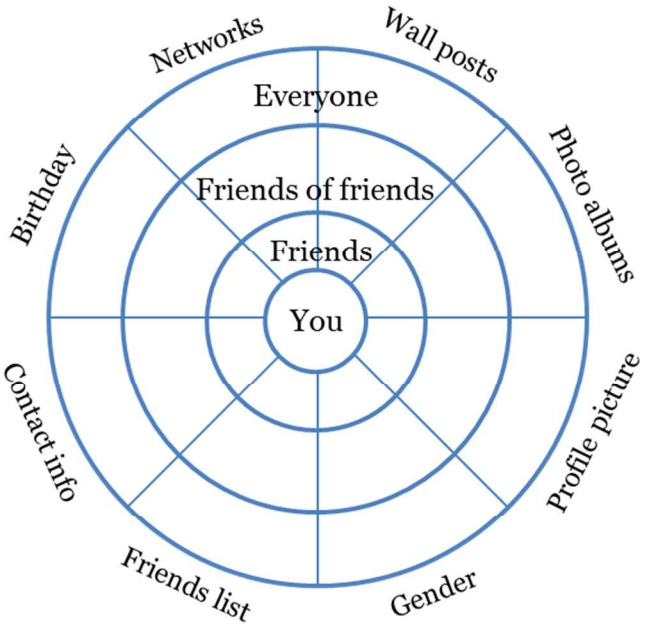


Figure 3. Visualization of the Granularity of Privacy Control Features

Summarizing this literature, an increase in privacy control features should cause consumers to spend more effort learning to use the privacy controls and more time actually specifying each of their privacy decisions. Formally stated, we predict the following:

> *H2: As the level of privacy control features that are perceived as beneficial to consumers increases, consumers' perceived ease-of-use of the privacy controls decreases.*

Consumer Weighting of Capability and Ease-of-Use over Time

The primary contribution of feature fatigue theory is that it accounts for the differential effects of capability and ease-of-use before and after product usage. It assumes that perceived capabilities will cause an increase in expected utility before product usage and an increase in *experienced* utility (see Figure 1) after product usage over time. Similarly, expected ease-of-use improves expected utility before usage and experienced utility after usage. However, consumers provide different weights to these two factors before and after usage. Meaning, while both capability and ease-of-use have positive effects on utility and usage, the strength of the relationship reverses over time.

This utility reasoning is based on behavioral economics research that explains bounded rationality in consumers (Loewenstein and Prelec 1992). Specifically, when consumers evaluate options for distant future usage, they prefer options that are highly desirable (e.g., capability), but less feasible (e.g., ease-of-use). However, in the near future, this relationship is reversed—explaining why one-off studies can result in incorrect long-term conclusions. Near future events are perceived as more concrete than abstract, causing feasibility to be favored over desirability (Liberman and Trope 1998). In order for this phenomenon to fit the privacy control context, consumers must be able to evaluate privacy controls before usage. Although OSNs do not advertise their privacy controls before account creation, consumers can download an app or create an account and examine the privacy controls before using them with only the time cost of doing so.

However, the *experienced utility* construct can be narrowed down in the privacy control context. Gaining utility from privacy controls means that consumers were able to use the controls successfully to reach the settings they desire. Similarly, *expected utility* is the consumers' estimate or belief that the controls will help them successfully reach the settings they desire. Therefore, with this minor modification, we predict the following:

H3: Privacy control capability plays a larger role in consumers' expected utility (before use) than in their successful privacy control usage (after use).

H4: Privacy control ease-of-use plays a smaller role in consumers' expected utility (before use) than in their successful privacy control usage (after use).

Methodology

As noted, one of the difficulties of researching information privacy controls—particularly with OSNs—is the task of collecting both actual consumer behavior along with experimental manipulation for establishing causality. To address this research gap, we consequently created a mobile app-based geocaching game that also included a website application and an online social network that players were incented to create and use. Participants included 568 undergraduates at a private university in the US.

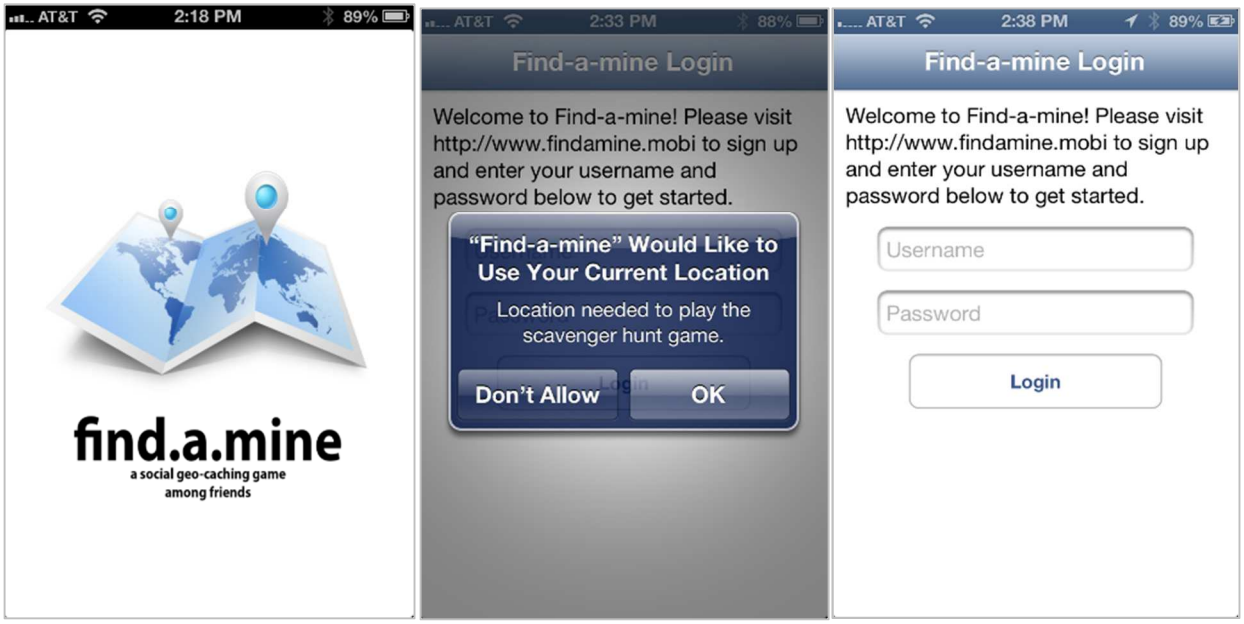
Geocaching is the sport of finding "treasures" (e.g. small objects, lists of finders, etc.) stored or "cached" in various geographic locations. Players use a GPS to find the caches. The mobile app (called "findamine" or "find.a.mine") was available in both the Apple App Store™ and Google Play™. Findamine was created as a modified geocaching game in which players took pictures of themselves at the locations rather than finding small objects. In addition, rather than providing a latitude/longitude coordinate, players were given short, text-based clues which lead to the locations (e.g., "This building was built in 1973.") or using the "hot-cold" meter that told them how close or far away they were from a site based on the real-time GPS coordinates provided by the player's device.

Each week (for 12 weeks), players received three new clues on their phone or tablet (iOS and Android supported) through the mobile app. Participants opened the clues and attempted to decipher the location. Once participants travelled to a clue location, they were prompted to take a picture on the mobile app at that location through a "Found It!" button. This photo was posted to the site along with the earned points. Participants could view their points on a web site "Leaderboard" in comparison to others (see Figure 4 and 5 for examples).

Participants also earned points by sharing demographic information and uploading a photo on the personal profile they created on the website, referring friends to join. Perhaps most relevant to our study, players were also awarded points for adding friends to their findamine social network. The findamine social network consisted of *frenemies* (other players to track and message with) and *minions*. Minions were players that were referred after the game began. Players were awarded a percentage (which increased as the number of minions increased) of their minion's overall points as incentive to build their social network.

We provided weekly and end-of-game incentives to encourage play. Each week, we awarded 3-15 gift cards ($10 Visa) 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 highest total points won a Google Nexus™ tablet. We also held a random drawing, based on points earned, to award a third Google Nexus™.

a. Splash screen b. Location data disclosure c. Login screen



d. Clue selection e. Clue begins f. Clue found

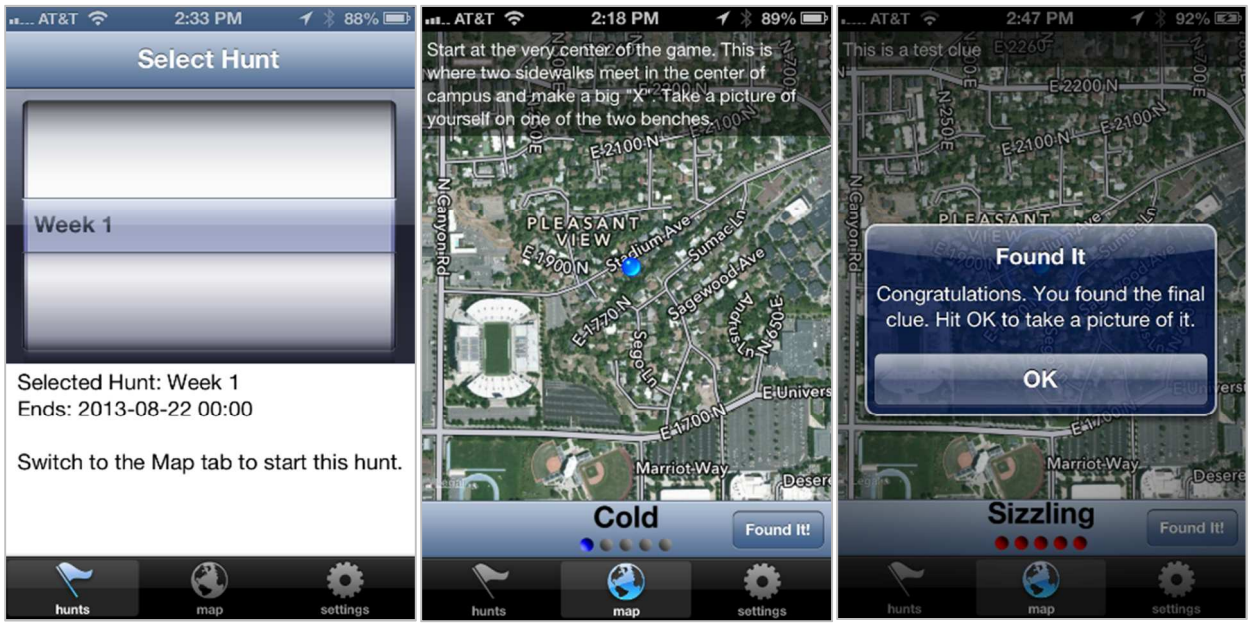


Figure 4. Mobile Screen Shots

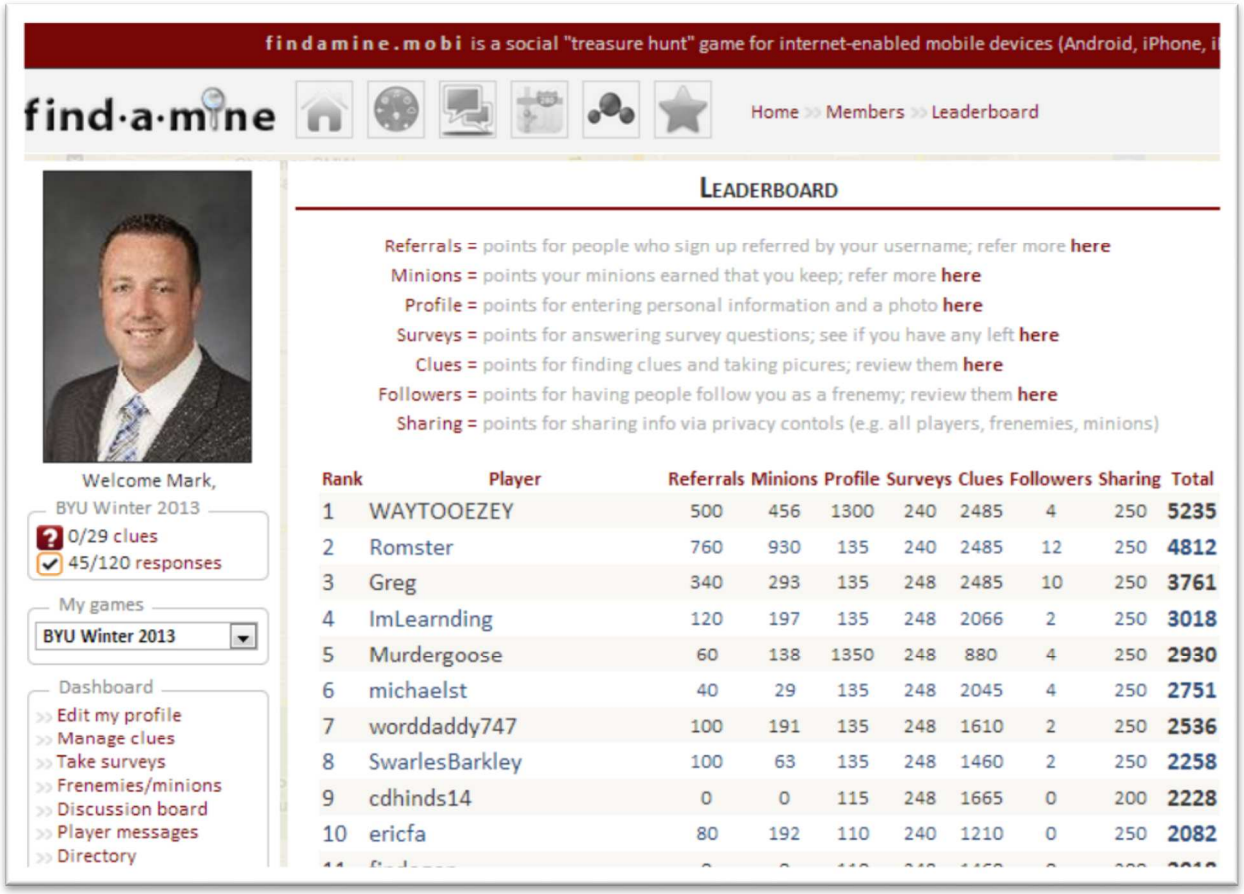


Figure 5. Game Leaderboard (website view)

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 waive participants' informed consent because this would elevate 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 (Fisher 1993). 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 an obvious need to collect location data, which presents personal safety risks (Thompson et al. 2012). The social network aspect of the app created both additional enjoyment as well as creating vertical and horizontal personal information privacy risks (Posey et al. 2010). The website included a player directory and social network. 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 as frenemies to their social network. Thus, participants' personal information could legitimately be made public—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.

Experimental Manipulation

To understand how the antecedents of privacy control expectations and usage change over time, we created a manipulation within the app code to randomly assigned players (as they registered) to one of three privacy control conditions (see Figure 6) based on low, medium, or high complexity/granularity.

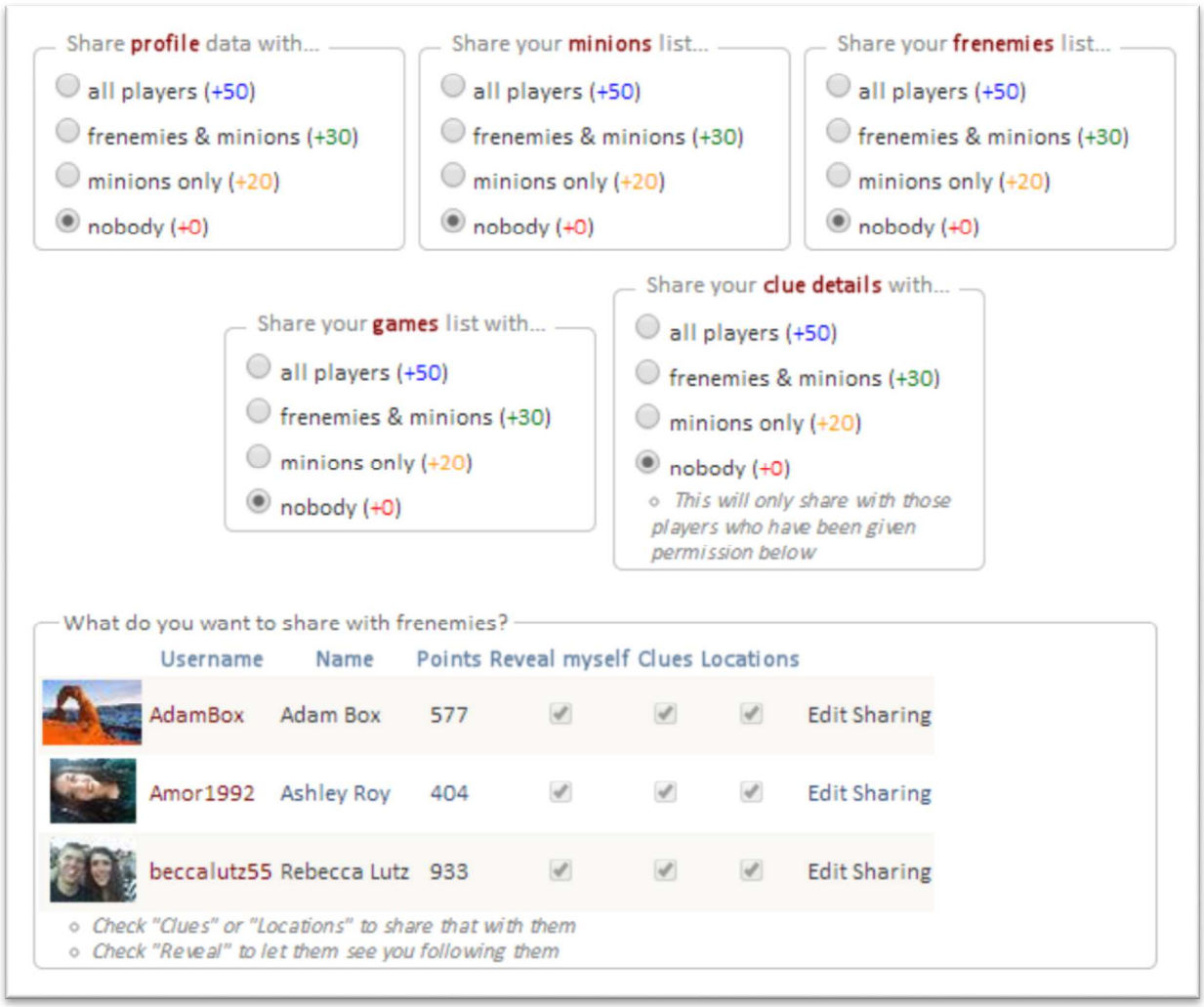


Figure 6. Example of Privacy Control "High" Complexity Treatment

The Low condition gave players the option to share all types of information with 1) nobody, 2) minions only, 3) minions and frenemies, or 4) everyone (1 type x 4 groups = 4 options). The Medium condition allowed players to specify which types of information (clues, profile, minions list, frenemy list, game list) each group could access (5 types x 4 groups = 20 options). The High condition allowed players all the options of the Medium condition plus the ability to further specify the information shared with each specific alter (frenemy) in their social network. If the player had 10 social network frenemies, then they would have 50 privacy control options to select from ((5 types x 4 groups) + (10 frenemies x 3 options)).

Measures

Because of our research design, we were able to capture a variety of objective measures in addition to the actual privacy settings—as opposed to the typical slate of self-reported perceptual measures. In particular, we measured the disclosure of profile data, clue locations, frenemies, and minions. These control variables influence the players' selected privacy control settings. In addition to the game measures, we collected latent construct measures of perceived privacy control feature complexity/granularity, control capability, control ease-of-use, expected privacy control utility, privacy concern, and self-efficacy. These measures were drawn from prior research but adapted for the privacy control context (Keith et al. 2011; Thompson et al. 2005; Xu et al. 2012a).

Procedures

A total of 568 participants were recruited from a course required as a pre-requisite for all business school majors. After removing those with incomplete data, 441 valid participants remained. They were given a document at the beginning of the semester, which instructed them to navigate to the findamine.mobi website, register for a player's account, and adjust their privacy settings. Again, participants were deceived to believe that they were helping to Beta test the app. Therefore, when the participants navigated to the privacy controls after registering, they were asked to answer a series of survey questions measuring the constructs listed above, on the understanding the information was used to help improve the app, not for research manipulation purposes. Next, the players were instructed that they must answer all survey questions and find at least six clues to receive the extra credit. All other game features (e.g., disclosing information, adjusting privacy settings, and referring friends) were optional and thus up to the participants to use as they normally would choose to do so in their natural interactions with apps. This allowed us to get a baseline of game data, yet allow realistic usage behaviors. At the end of the 12 weeks, survey questions appeared once again on the privacy settings screen and players were instructed to answer them once more to receive full credit. After the end of the game, the tablets were awarded.

Results

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 common methods bias (CMB). For brevity, the details are not reported here, but are fully available upon request. However, the results indicated acceptable factorial validity and minimal multicollinearity based on the standards for Information Systems research (Gefen and Straub 2005; Liang et al. 2007; Pavlou et al. 2007; Straub et al. 2004). CMB was assessed using both Harmon's single factor approach as well as the unrelated latent marker construct technique, both methods indicating minimal bias (Liang et al. 2007; Podsakoff et al. 2003; Richardson et al. 2009). However, recent research (Chin et al. 2012) indicates that these methods are not entirely reliable indicators of a lack of CMB. Perhaps the best evidence for this data is the fact that each latent construct was measured at varying times and never in a single "session." Rather, participants answered survey items as the clues they were attached to were released each week.

Hypothesis Testing

To analyze the results, we developed a path model with the PLS Structural Equation Modeling technique using SmartPLS 2.0.M3 (Ringle et al. 2005). Use of this analytical approach was appropriate because 1) we needed to test multiple paths in the same model; 2) privacy concern was modeled as a second-order formatives; and, 3) PLS does not depend on normal distributions or interval scales (Chin et al. 2003; Fornell and Bookstein 1982)—making it ideal for our objective measures of game play behavior. 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 to earn points, it originated in an information systems course that was dominantly male.

	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 visits (sessions):	Total $\bar{x}$ = 9.90 Mobile $\bar{x}$ = 3.90	Total $\bar{x}$ = 4.79 Mobile $\bar{x}$ = 1.43

Table 1. Descriptive Statistics

Table 2 summarizes the variable means, standard deviations, and construct correlations. Figure 7 visualizes 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=411). R^2 values represent the amount of total variance accounted for by the exogenous variables.

Before:

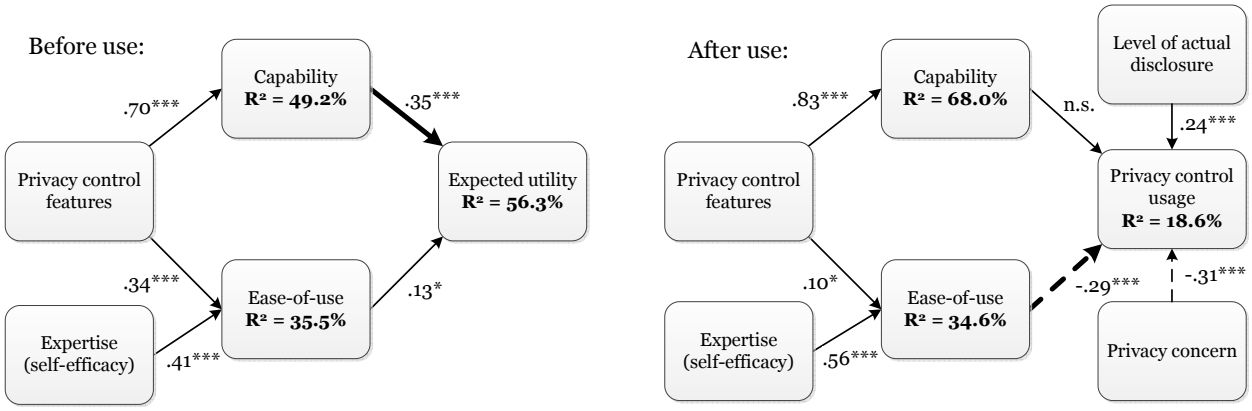
Var.	x̄	s	1	2	3	4	5	6
1 Cap	4.6	1.3						
2 Comp	4.5	1.6	.70					
3 Expt Ut	5.0	1.4	.69	.68				
4 Exper.	5.5	1.4	.34	.26	.18			
5 PC	4.7	1.3	.00	-.11	-.02	.12		
6 Profile	126.8	29.8	.05	-.02	-.04	.11	.22	
7 EOU	4.9	1.4	.71	.44	.51	.50	-.01	-.01

After:

Var.	x̄	s	1	2	3	4	6	7
1 Cap	4.6	1.2						
2 Comp	4.6	1.4	.82					
3 Expd Ut	468.5	87.8	-.04	.00				
4 Exper.	5.5	1.4	.16	.18	.11			
6 PC	4.7	1.3	.09	-.03	-.27	.02		
7 Profile	126.8	29.8	.04	.05	.17	.05	.18	
8 EOU	4.9	1.4	.22	.20	-.12	.58	.03	.10

Note: Cap = Control Capability, Comp = Control Complexity (aka features), Expct Ut = Expected Utility, Expd Ut = Experienced Utility (higher means more sharing), Exper. = Expertise (self-efficacy), PC = Privacy Concern, Profile = amount of profile data disclosed (level of actual disclosure), EOU = Ease-of-use

Table 2. Construct Correlations



n.s. = not supported statistically, *=p<.05, **=p<.01, ***=p<.001

Figure 7. Path Coefficients and R Squared Values for Hypothesis Testing

To compare the effect of capability on expected utility (before use) to the effect on privacy control usage (after use), we cannot simply compare the β coefficients as they are not surrogates for effect size. Rather, we simply compare the Pearson correlation coefficients. As such, the correlation before use (0.69) is certainly higher than the correlation after use (-.04). Similarly, the correlation of ease-of-use before use (.51) is much higher than after use (-.12).

Discussion

Overall, the PLS analysis results support the main tenets of privacy fatigue theory. However, there were some unexpected findings worth noting. As expected, the perceived complexity and granularity of the privacy control features had a significant impact on perceived control capability both before use ($\beta = 0.702$, $p < 0.001$) and after use ($\beta = 0.825$, $p < 0.001$); thus, confirming H1. Perceived features also had a significant effect on perceived ease-of-use before use ($\beta = 0.339$, $p < 0.001$) and after use ($\beta = 0.102$, $p < 0.05$). However, the direction was positive rather than negative as hypothesized (discussed later).

H3 was also confirmed. Perceived privacy control capabilities was a significant indicator of expected utility before use ($\beta = 0.354$, $p < 0.001$), but not a significant predictor of actual privacy control usage (after use). Perceived ease-of-use was a significant indicator of expected privacy control utility before use ($\beta = 0.132$, $p = 0.05$). However, ease-of-use played a much larger in determining actual privacy control usage ($\beta = -0.293$, $p < 0.001$). In this case, the result does not indicate a negative relationship, but that the more usable the controls, the more likely participants were to adjust the privacy control settings "downward" (make them more restrictive) from the default setting that allowed sharing with all players. Finally, each of the control variables was significant in the privacy fatigue model. Privacy concern caused participants to further restrict their privacy control settings ($\beta = -0.31$, $p < 0.001$). Those who submitted more personal information (profile data, location data, social network data) were more likely to loosen their privacy settings ($\beta = 0.242$, $p < 0.001$).

Implications to Research and Practice

The primary contribution of this research is the application of feature fatigue theory into the information privacy control context. Overall, our results reveal a very similar effect as was found with traditional consumer products: product feature capabilities play a larger role in pre-usage/purchase perceptions whereas product feature ease-of-use plays a larger role after usage over time. This phenomenon exists because consumers discount product feasibility when considering long term usage (Liberman and Trope 1998).

The practical implication of privacy fatigue is noteworthy. If OSNs opt to set consumer default privacy settings to more "relaxed" standards and simultaneously employ complex privacy settings, they can clearly cause consumers to accept more information disclosure than the consumers may be comfortable with—simply because of the lack of control ease-of-use. The danger of this practice to consumers is that before usage, these complex privacy controls are highly desirable to users and give them the perception that the OSN is providing them with a relatively preferable option for managing privacy. Therefore, consumers are likely to be more tempted and ensnared by OSN providers who design complex privacy controls with the intention of encouraging greater information disclosure.

This trap for OSN consumers is magnified by the finding that greater privacy control complexity and granularity actually leads to greater perceived ease-of-use. That is, consumers believe such controls will be easier to learn and to use. This effect may not be particularly surprising in the privacy control context. Unlike a DVD player where only a few options are needed to perform the necessary functions, a privacy control feature that does not allow for the granularity necessary to share information with only those intended reduced its ease-of-use in the mind of the consumer. Evidence of this can be found in technology acceptance research where perceived ease-of-use affects the perceived usefulness of a technology (Venkatesh et al. 2003).

Further analysis of the positive effect of privacy control complexity on ease-of-use revealed an interesting finding with our data. Those in the Medium complexity treatment perceived greater ease-of-use than the Low treatment, yet *more* than the High treatment (see Figure 8). As granularity is decreased, ease-of-use should increase. Therefore, the ease-of-use measured may more accurately reflect the users' desire for expressiveness, or the ability of the user to express exact preferences. The "negative" effect observed with ease-of-use then may actually relate to the user's desire for expressiveness.

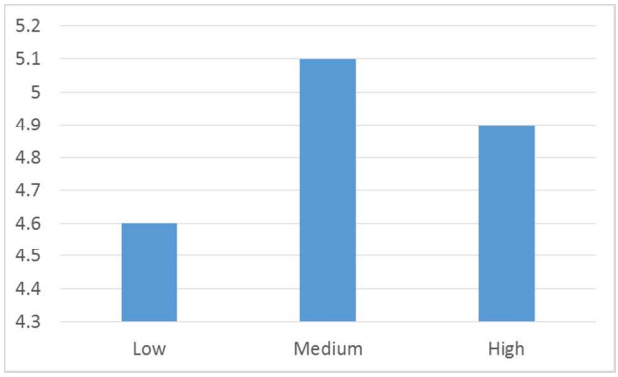


Figure 8. Privacy Control Complexity Treatment by Ease-of-Use

As noted in the previous section, we found a positive relationship between information disclosure and loosened privacy settings. While this is an intriguing and seemingly counterintuitive finding, we believe this might be unique to our Findamine game context. Users were directly incented with points to make information available. Therefore, in this context, the relationship could be positive because people wanted to earn more points by disclosing and sharing information rather than keep their information private. In other situations, this effect would probably not exist. Of course, these and other explanations require additional research.

Another key contribution of this research is our field experiment methodology. The combination of a longitudinal study with both experimental manipulation and the collection of actual user behavior is unique in the field of privacy control research. Although this methodology is not without its limitations, by employing experimental manipulation in a field setting, we strengthened the study's internal and external validity.

Limitations and Future Research

Although every effort was made in this study to create an experimental procedure that is both internally and externally valid, several limitations exist in our study that point to compelling future research opportunities. For example, the game context of the Findamine OSN may not represent the majority of OSN contexts. For example, the purpose of Facebook and Twitter is to share information among friends for social benefits while Findamine was intended to allow participants to share information about the game and competition they were sharing. Thus, as some OSNs provide Application Programming Interfaces to work tightly within the OSN, this may be an alternative future direction to improve our understanding of feature fatigue within a much broader context.

By recruiting participants from a university course rather than allowing the OSN adoption to happen organically through social channels, we may have gathered a sample that is unrepresentative of the most OSN populations. To counter balance this possibility, the pool of participants was given the option to complete a variety of extra credit opportunities for the same benefit. They were encouraged to select the activity that most interested them. Additionally, the participants could refer other friends to play (which many did) to make the context more relevant to their interests.

Perhaps most important, our context did not allow participants to choose among various privacy control options. Rather we traded this for the ability to manipulate privacy control treatments in order to establish causality. This is not so much a limitation to external validity since most consumers to make OSN usage decisions on other factors rather than the complexity of privacy controls. This is more of a limitation of the adaptation of feature fatigue theory to the privacy control context. This is not to say that feature fatigue is unusable. Rather, future research should adapt privacy fatigue theory to this unique assumption.

Conclusion

The opportunity for secondary information use can be profitable for companies. Studying the manipulation of privacy control complexity to extract information from users is not only a step forward in

information privacy theory but also weighty to companies gathering and sharing user information. This research contributes a modified feature fatigue model in the context of privacy controls. Our empirical results and unique research methodology provide strong, yet still preliminary, support of privacy fatigue theory. This study can help design science research by guiding the intentions of the privacy control design.

References

Acquisti, A., and Gross, R. 2006. "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook," *Privacy enhancing technologies*: Springer, pp. 36-58.

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.

Ayalon, O., and Toch, E. 2013. "Retrospective Privacy: Managing Longitudinal Privacy in Online Social Networks," *Proceedings of the Ninth Symposium on Usable Privacy and Security*: ACM, p. 4.

Bandura, A. 2001. "Social Cognitive Theory: An Agentic Perspective," *Annual review of psychology* (52:1), pp 1-26.

Bankston, K. 2009. "Facebook's New Privacy Changes: The Good, the Bad, and the Ugly."

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

Benisch, M., Kelley, P.G., Sadeh, N., and Cranor, L.F. 2011. "Capturing Location-Privacy Preferences: Quantifying Accuracy and User-Burden Tradeoffs," *Personal and Ubiquitous Computing* (15:7), pp 679-694.

Brandimarte, L., Acquisti, A., and Loewenstein, G. 2013. "Misplaced Confidences Privacy and the Control Paradox," *Social Psychological and Personality Science* (4:3), pp 340-347.

Brooke, J. 1996. "Sus-a Quick and Dirty Usability Scale," *Usability evaluation in industry* (189), p 194.

Calero, C., Ruiz, J., and Piattini, M. 2005. "Classifying Web Metrics Using the Web Quality Model," *Online Information Review* (29:3), pp 227-248.

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.

Chin, W.W., Thatcher, J.B., and Wright, R.T. 2012. "Assessing Common Method Bias: Problems with the Ulmc Technique," *MIS Quarterly* (36:3), pp 1003-1019.

Choi, S.S., and Choi, M.-K. 2007. "Consumer's Privacy Concerns and Willingness to Provide Personal Information in Location-Based Services," *The 9th International Conference on Advanced Communication Technology*: IEEE, pp. 2196-2199.

Debatin, B., Lovejoy, J.P., Horn, A.K., and Hughes, B.N. 2009. "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences," *Journal of Computer-Mediated Communication* (15:1), pp 83-108.

Dey, R., Jelveh, Z., and Ross, K. 2012. "Facebook Users Have Become Much More Private: A Large-Scale Study," *4th IEEE Annual Workshop on Security and Social Networking*: IEEE, pp. 346-352.

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

Emerson, R.M. 1976. "Social Exchange Theory," *Annual Review of Sociology* (2), pp 335-362.

Fisher, R.J. 1993. "Social Desirability Bias and the Validity of Indirect Questioning," *Journal of Consumer Research* (20:2), pp 303-315.

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.

Gross, R., and Acquisti, A. 2005. "Information Revelation and Privacy in Online Social Networks," *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*: ACM, pp. 71-80.

Guo, S., and Chen, K. 2012. "Mining Privacy Settings to Find Optimal Privacy-Utility Tradeoffs for Social Network Services," *2012 International Conference on Privacy, Security, Risk and Trust (PASSAT) and 2012 International Conference on Social Computing (SocialCom)*: IEEE, pp. 656-665.

Hargittai, E. 2010. "Facebook Privacy Settings: Who Cares?," *First Monday* (15:8).

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.

Hornbæk, K. 2006. "Current Practice in Measuring Usability: Challenges to Usability Studies and Research," *International Journal of Human-Computer Studies* (64:2), 2//, pp 79-102.

Hui, K.L., Teo, H.H., and Lee, S.Y.T. 2007. "The Value of Privacy Assurance: An Exploratory Field Experiment," *MIS Quarterly* (31:1), pp 19-33.

Ibrahim, S.Z., Blandford, A., and Bianchi-Berthouze, N. 2012. "Privacy Settings on Facebook: Their Roles and Importance," *2012 IEEE International Conference on Green Computing and Communications (GreenCom)*: IEEE, pp. 426-433.

Joinson, A.N. 2008. "Looking at, Looking up or Keeping up with People?: Motives and Use of Facebook," *Proceedings of the SIGCHI conference on Human Factors in Computing Systems*: ACM, pp. 1027-1036.

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.

Lancaster, K. 1971. *Consumer Demand: A New Approach*. New York: Columbia University Press.

Langer, E.J. 1975. "The Illusion of Control," *Journal of personality and social psychology* (32:2), p 311.

Lewis, K., Kaufman, J., and Christakis, N. 2008. "The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network," *Journal of Computer-Mediated Communication* (14:1), pp 79-100.

Li, Y. 2012. "Theories in Online Information Privacy Research: A Critical Review and an Integrated Framework," *Decision Support Systems* (54:1), pp 471-481.

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

Liberman, N., and Trope, Y. 1998. "The Role of Feasibility and Desirability Considerations in near and Distant Future Decisions: A Test of Temporal Construal Theory," *Journal of Personality and Social Psychology* (75:1), p 5.

Liu, Y., Gummadi, K.P., Krishnamurthy, B., and Mislove, A. 2011. "Analyzing Facebook Privacy Settings: User Expectations Vs. Reality," *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*: ACM, pp. 61-70.

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

Lowry, P.B., Cao, J., and Everard, A. 2011. "Privacy Concerns Versus Desire for Interpersonal Awareness in Driving the Use of Self-Disclosure Technologies: The Case of Instant Messaging in Two Cultures," *Journal of Management Information Systems* (27:4), pp 165-204.

Madejski, M., Johnson, M., and Bellovin, S.M. 2012. "A Study of Privacy Settings Errors in an Online Social Network," *2012 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM)*: IEEE, pp. 340-345.

Mai, B., Menon, N.M., and Sarkar, S. 2010. "No Free Lunch: Price Premium for Privacy Seal-Bearing Vendors," *Journal of Management Information Systems* (27:2), Fal, pp 189-212.

Meeder, B., Tam, J., Kelley, P.G., and Cranor, L.F. 2010. "Rt@ Iwantprivacy: Widespread Violation of Privacy Settings in the Twitter Social Network," *Proceedings of the Web 2.0 Privacy and Security Workshop*.

Mick, D.G., and Fournier, S. 1998. "Paradoxes of Technology: Consumer Cognizance, Emotions, and Coping Strategies," *Journal of Consumer Research* (25:2), pp 123-143.

Mukherjee, A., and Hoyer, W.D. 2001. "The Effect of Novel Attributes on Product Evaluation," *Journal of Consumer Research* (28:3), pp 462-472.

Netter, M., Riesner, M., Weber, M., and Pernul, G. 2013. "Privacy Settings in Online Social Networks--Preferences, Perception, and Reality," *Proceedings of the Hawaii International Conference on System Sciences*: IEEE, pp. 3219-3228.

Nielsen, J. 1994. "Usability Inspection Methods," *Conference companion on Human factors in computing systems*: ACM, pp. 413-414.

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

Podsakoff, P.M., MacKenzie, S.B., Lee, J.-Y., and Podsakoff, N.P. 2003. "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies," *Journal of applied psychology* (88:5), p 879.

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

Richardson, H.A., Simmering, M.J., and Sturman, M.C. 2009. "A Tale of Three Perspectives: Examining Post Hoc Statistical Techniques for Detection and Correction of Common Method Variance," *Organizational Research Methods*).

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

Sadeh, N., Hong, J., Cranor, L., Fette, I., Kelley, P., Prabaker, M., and Rao, J. 2009. "Understanding and Capturing People's Privacy Policies in a Mobile Social Networking Application," *Personal and Ubiquitous Computing* (13:6), pp 401-412.

Smith, H.J., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* (35:4), pp 989-1016.

Stone, E.F., Gardner, D.G., Geuetal, H.G., and McClure, S. 1983. "A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes across Several Types of Organizations," *Journal of Applied Psychology*), pp 459-468.

Straub, D., Boudreau, M.-C., and Gefen, D. 2004. "Validation Guidelines for I.S. Positivist Research," *Communications of the Association for Information systems* (13), pp 380-427.

Stutzman, F., Gross, R., and Acquisti, A. 2013. "Silent Listeners: The Evolution of Privacy and Disclosure on Facebook," *Journal of Privacy and Confidentiality* (4:2), p 2.

Thompson, D.V., Hamilton, R.W., and Rust, R.T. 2005. "Feature Fatigue: When Product Capabilities Become Too Much of a Good Thing," *Journal of Marketing Research* (42:4), 2005/11/01, pp 431-442.

Thompson, S., Keith, M.J., and Posey, C. 2012. "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)*, Provo, Utah, USA, p. 25.

Venkatesh, V., Morris, M.G., Davis, G.B., and Davis, F.D. 2003. "User Acceptance of Information Technology: Toward a Unified View," *MIS Quarterly* (27:3), Sep, pp 425-478.

Walrave, M., Vanwesenbeeck, I., and Heirman, W. 2012. "Connecting and Protecting? Comparing Predictors of Self-Disclosure and Privacy Settings Use between Adolescents and Adults," *Cyberpsychology* (6:1).

Wiklund, M.E. 1994. *Usability in Practice: How Companies Develop User-Friendly Products*. New York: Academic Press.

Williams, J., Feild, C., and James, K. 2011. "The Effects of a Social Media Policy on Pharmacy Students' Facebook Security Settings," *American journal of pharmaceutical education* (75:9).

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

Xu, H., Teo, H.-H., Tan, B.C.Y., and Agarwal, R. 2012b. "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), April 18, 2012, pp 1342-1363.

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.

Ziefle, M. 2002. "The Influence of User Expertise and Phone Complexity on Performance, Ease of Use and Learnability of Different Mobile Phones," *Behaviour & Information Technology* (21:5), pp 303-311.