Provided for non-commercial research and education use.
Not for reproduction, distribution or commercial use.

This article appeared in a journal published by Elsevier. The attached copy is furnished to the author for internal non-commercial research and education use, including for instruction at the authors institution and sharing with colleagues.

Other uses, including reproduction and distribution, or selling or licensing copies, or posting to personal, institutional or third party websites are prohibited.

In most cases authors are permitted to post their version of the article (e.g. in Word or Tex form) to their personal website or institutional repository. Authors requiring further information regarding Elsevier's archiving and manuscript policies are encouraged to visit:

http://www.elsevier.com/copyright

Author's personal copy

Computers in Human Behavior 28 (2012) 1019–1027

Contents lists available at SciVerse ScienceDirect

Computers in Human Behavior

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

Affect, cognition and reward: Predictors of privacy protection online

Yong Jin Park [a,*], Scott W. Campbell [b], Nojin Kwak [b]

[a] School of Communications, Radio, Television, and Film, Howard University, 3735 Mazewood Lane, Fairfax, VA 22033, USA
[b] Department of Communication Studies, University of Michigan, USA

ARTICLE INFO

Article history:
Available online 29 January 2012

Keywords:
Information control
Privacy protection
Internet surveillance
Knowledge

ABSTRACT

This article examined the interplay between cognition and affect in Internet uses for privacy control. A survey of a national sample was conducted to empirically test the relationship between affective concern for and cognitive knowledge of information privacy online. We also tested for the interactive role of reward-seeking as a moderator among these relationships. Findings revealed that concern did not directly play a meaningful role in guiding users' protective behavior, whereas knowledge was found significant in moderating the role of concern. The interactive role of reward-seeking seems particularly salient in shaping the structure of the relationships. These findings suggest that the intersections between knowledge, reward, and concern can play out differently, depending on the levels of each. Policy implications in relation to users' cognitive, affective, and reward-seeking rationalities are offered, and future research considerations are discussed.

© 2012 Elsevier Ltd. All rights reserved.

1. Introduction

The duality of cognition and emotion is a central pole of decision making and social behavior. On one hand, emotion serves as functional guidance as people resort to anger, fear, happiness, and trust for behavioral direction. On the other hand, people take a cognitive route, modifying thinking and rationality, to control their behavior. To illustrate, scholars of political psychology have long recognized this dual dynamic and its role in voting behavior and political judgment (Just, Crigler, & Neuman, 1998; Marcus, Neuman, & Mackuen, 2000). Yet with regard to behavior online, particularly sharing and protecting personal data, systematic understanding of affective appraisal and cognitive processing has only recently begun to emerge.

This study draws from research and theory on the dynamic interplay between affect and cognition to help untangle an emergent paradox regarding Internet privacy – namely, the incongruence between privacy concern and users' inaction in managing personal information online. The central question here is whether knowledge about privacy matters moderates one's level of concern about sharing personal information online to encourage or curtail active information control. Of particular interest is the interactive relationship between privacy knowledge (cognitive dimension) and one's level of concern (affective dimension) over websites and organizational entities collecting personal information online. Because personal data are oftentimes gathered in exchange for rewards (e.g., free gifts or access to content), this study also examines how reward functions as a moderating variable, along with concern and knowledge, in predicting active measures of privacy protection.

This project has theoretical as well as practical policy implications. On the theoretical front, to merge insights from political communication to the field of information privacy is to newly advance understandings of user psychology from affective as well as cognitive perspectives of Internet surveillance. On the policy front, this study helps identify the source of behavioral disjuncture among the concerned public and provide much needed empirical evidence to better inform policymakers about user rationality. A national survey based on probability sampling offers an opportunity to empirically test the interplay between affect and cognition in a diverse and representative online user population in the US.

Noted scholars (Acquisti & Grosslags, 2005; Boyd & Hargittai, 2010; Turow, 2003; Turow, Feldman, & Meltzer, 2005) are in fact rapidly incorporating the distinctive role of cognitive power in various uses of the Internet and privacy. Despite their systematic efforts, empirical evidence is scant as to how and to what extent privacy knowledge plays a role in personal information control online while accounting for affective elements and rewards offered for sharing personal data. In the following sections, this study starts with a theoretical discussion, leading to testable hypotheses and a research question in the prospect of theoretical refinement. Then, we analyze the complex interplay between affect, knowledge, and reward in predicting reported levels of privacy protection online and offer conclusions to help with policy judgments and future research.

* Corresponding author. Tel.: +1 703 657 2181.
E-mail address: yongjinp@hotmail.com (Y.J. Park).

0747-5632/$ - see front matter © 2012 Elsevier Ltd. All rights reserved.
doi:10.1016/j.chb.2012.01.004

Author's personal copy

2. Affect, cognition and behavior

2.1. Affective route

People rely on feelings to make strategic decisions. Fear, anxiety or worry – and their counterpart trust – serve as a triggering platform for ordinary people to react (Marcus et al., 2000; Neuman, 1991). In the domain of information control, the concern over technological surveillance is a common reason why users are expected to be fully engaged in control behavior. Much of the literature that addresses anxiety about surveillance starts with the assumption of affective congruence in which emotional concern and cues activate users with protective behavior that corresponds with their levels of trust or anxiety. In fact, however, scholars are faced with an apparent paradox – that is, increased concern in a virtual environment does not necessarily translate into protective actions.

There are consistent research findings (Acquisti, 2004; Acquisti & Grosslags, 2005; Goldman, 2003; Khalifa & Limayem, 2003; Park, 2008; Turow & Hennessy, 2007; Turow et al., 2003) that indicate the incongruence between privacy concern and actual information behavior. At best, scholars have found only a weak positive relationship between concern and privacy protection (Acquisti & Grosslags, 2005; Culnan, 1995), while others have actually found an inverse relationship between the two (Chen & Rea, 2004), suggesting that sometimes users are less concerned when they take protective actions. These mixed findings are noteworthy considering in mass media psychology emotional cues are thought to be quite functional in guiding behavior and strategic choices. Indeed, it is logical to assume that more concerned or anxious individuals are more likely to elicit a behavioral response to a threatening environment or stimulus (MacLeod & Mathews, 1988). Yet, as noted above, this does not seem to translate well into users protecting personal data online.

2.2. Cognitive route

Note that the behavioral effect of affective appraisal is sometimes exclusively privileged in common expectations of user information behavior; simply put, negative affect *should* lead to protective action. However, emotions alone may not lead to time consuming and costly information management in a systematic fashion. In other words, we do not always find ourselves in the domain of emotional contexts that are sufficient to guide strategic management of conditions. Instead, scholars have suggested heuristic inaction is likely to hold when the mode of explicit consideration is unavailable in unfamiliar territories of cyberspace (Acquisti & Grosslags, 2005; Neuman, 1991). In this regard, a high level of concern, coupled with a lack of knowledge, may not function as an explicit route for the affective state to result in carefully-deliberate organized actions (Ajzen, 1991; Dietrichson, 2001; Downs, 1957).

Here one of Erving Goffman's premises about social behavior provides a point of reference. Decades ago, Goffman (1965) posited that humans perform private–public boundary management by selectively revealing the self. A strong causal assumption is that individuals possess critical understandings of the surrounding environment and its implicit rules before being able to take appropriate actions. In other words, actions are aided by social knowledge. Empirical evidence, however, has been elusive despite the existing and growing interest in user knowledge. On one hand, it has been found that knowledge is a prerequisite for tangible action and certain skill (Eveland, Hayes, Shah, & Kwak, 2005, for political participation Hargittai, 2004, 2008; Tai, Egelman, Cranor, & Acqusti, 2007). On the other hand, information may dampen careful deliberation, as more knowledge is in fact sometimes related to less concern (Dommeyer & Gross, 2003; Uslaner, 2004).

2.3. Interplay between affect and cognition

Thus, it is difficult to predict exactly how knowledge about information privacy will moderate one's affective orientation toward online surveillance. Yet there are theoretical grounds for anticipating an interaction between the two in predicting privacy behavior, considering the dual system of emotion and cognition in human information processing works in a delicate interactive dynamic. For example, drawing upon insights from neurosciences, Marcus and his colleagues (Marcus et al., 2000) posit that individuals use two separate systems of emotion and cognition, not in isolation, but in interplay, to monitor the environment for signals of well being or threats (Just et al., 1998; Marcus et al., 2000).

Beyond the overarching hypothesis that cognition (in this case privacy knowledge) will moderate affect (in this case concern) in predicting privacy protection, we advance and test the following two alternative theoretical scenarios about the nature of the interaction between the two. First, it is conceivable that knowledge about Internet privacy will emerge as the "missing link" between concern over privacy protection and (in)action in this regard. That is, one might anticipate that those who are least trusting about the privacy of their personal data are most motivated to protect those data when they are knowledgeable about how personal data are collected online and what they are used for. In this case, knowledge serves as a reinforcing mechanism for those who are most concerned about their privacy to take action. On the other hand, it is possible that privacy knowledge primarily benefits those who are least concerned about their privacy. In this case, increased knowledge about the collection and use of personal data online helps compensate for a lack of concern, leading to higher levels of personal data protection. Thus, each of these hypotheses will be tested by examining the moderating effect of knowledge on concern in predicting privacy behavior online.

3. Enticement and reward

In examining the underlying dynamics of the privacy paradox it is important to also recognize that users are often enticed into to making compromising transactions with their personal information. Scholars point out that it is not uncommon for individuals to give up personal information in exchange for content (Pastore, 1999), discounts (White, 2004), prizes (Earp & Baumer, 2003), and the like. In fact, reward plays such a prominent role in online behavior that scholars question whether it may be a primary reason why concerns about personal information do not translate into protective action. Yet, scholars found that participants *did* strategize to protect their identities during e-commerce transactions by withholding certain information and applying rules about what kind of data they would give up for a free reward (Metzger, 2007; Phelps, Nowak, & Ferrell, 2000). Furthermore, Turkle (1995) found that a majority of study respondents said they were unwilling to give up personal data for instant satisfaction while disapproving most scenarios in which websites potentially benefit users with collected data.

Thus, questions remain about the role of reward-seeking and cost–benefit analysis in privacy protection online. While many Internet users feel anxious and/or aware about surveillance (cost), many are willing to trade off their privacy for immediate rewards or gratifications (benefit) Acquisti, 2004; Acquisti & Grosslags, 2005. At the same time, there is also empirical evidence that users are conscious about the cost–benefit tradeoff in accepting those rewards (Turkle, 1995; Turow et al., 2003), giving us reason to expect that reward seeking will interact with one's levels of concern and knowledge in predicting their efforts to protect personal data. In all, it may still be plausible to suspect the negative role of reward-seeking, speculating that for those who are willing to provide

Author's personal copy

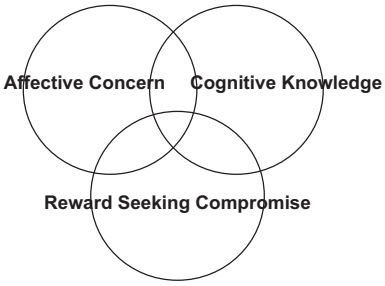

Fig. 1. Affective concern, cognitive knowledge, and reward-seeking.

personal data for benefits, knowledge may reinforce concern even more strongly; therefore, we pose questions instead of hypotheses in order to examine the nature of three-way interactions among concern, knowledge, and reward-seeking (see Fig. 1).

4. Hypotheses and research question

To summarize, this study is interested in the interactive relationships between affect, knowledge, and reward in predicting privacy protection behavior online. The literature and theory discussed above serve as a foundation for testing two alternative hypotheses about the moderating effect of knowledge on concern: The first (*H1a*) being that privacy concern will be more strongly associated with privacy protection for those with higher levels of knowledge than those with lower levels of knowledge. In this scenario, knowledge reinforces privacy concern. The alternative scenario (*H1b*) is that privacy knowledge primarily benefits those who are least concerned, thus a lack of concern will be more strongly associated with privacy protection for those with higher levels of knowledge. In this scenario, knowledge compensates for a void of concern.[1] The research question examines the nature of these interactions when reward-seeking is included as a third moderator. Thus, *RQ1* asks: What are the three-way interactions among concern, knowledge, and reward-seeking in predicting privacy protection online? Although we are primarily interested in the interactive effects of these predictor variables, we will also report on their direction associations with privacy protection in the analysis for baseline insights into the relative roles of each.

5. Methods

5.1. Sampling and data collection

The analysis is based on a national probability sample of adult Internet users (18 and older). An external survey firm recruited the panel respondents, using random digit dialing (RDD) on the sample frame of the entire US residential telephone numbers. The panel participants were asked to visit a site and complete an online survey. In order to improve response rate, an email reminder was sent to non-respondents after 3 days of the initial contact. The cross sectional data included only adult Internet users who had Internet access at home, eliminating the Web-TV based panel participants. In order to ensure the representativeness, the sample was drawn to reflect demographic distributions in the key Census areas: income, gender, age, and region. The survey was administered over a 2-week period in November, 2008.

The demographic characteristics of the sample are not far different from those of the general population reported in the US Census Bureau's 2007 American Community Survey (ACS). With respect to education attainment, the median education level for those 25 or older in both data sets is some college. Household income (the median in the ACS and the current study is $50,000–74,999 and $60,000–74,999, respectively), gender (female in the ACS and the sample is 52.4% and 53.6%) and age (the median age for those 18 or older in the ASC and the current study is 45–54 and 47, respectively) resembles the profiles of the general population. There is a slightly smaller percentage of white respondents in the sample (77%) than in the ACS (79%). The total sample size was 456 with the completion rate of 69% (456 interviews completed among 663 contacted). Although the 456 interviews were completed, the final dataset was limited to 419 after an item check to ensure the validity of responses.

5.2. Measures

5.2.1. Privacy knowledge

With regard to knowledge, studies have operationalized different dimensions, including (1) knowledge of data collection risk and (2) awareness of regulatory protection. This study includes both since it is reasonable to expect that conscious awareness of the positive (i.e., regulatory protection) may function differently than that of the negative (i.e., data collection risk) in predicting privacy behavior. For knowledge of data risk, seven true–false items were used to assess the extent of user awareness of related policy measures ensuring the safe flow of personal data online. For knowledge of regulatory protection, users were asked, on a total of eight true–false questions, of the extent of online data surveillance practices. Items in each dimension were adopted primarily from prior studies (Turow, 2003; Turow et al., 2005) and later combined to create additive indexes, with 1 assigned for the correct answers and 0 for all other answers ($M = 4.73$, $SD = 2.40$, Kuder-Richardson 20 reliability = .79, for dichotomous knowledge items of data collection risk; $M = 1.96$, $SD = 1.86$, Kuder-Richardson 20 reliability = .73, for dichotomous knowledge items of regulatory protection).

5.2.2. Privacy concern

Uslaner (2004) and Westin (1998) originally developed a set of Internet concern measures on a 5-point scale. The original measures by Westin were limited to observe the user concern in terms of generic entities, not capturing the level of anxiety in terms of specific surveillance aspects (Ribak & Turow, 2003). Furthermore, recent studies (Boyd & Hargittai, 2010; Kumaraguru & Cranor, 2005; Marcus, Neuman, & Mackuen, 2008) began to point out the need of a more sensitive scale to capture affect-emotion dimensions. In fact, Turow (2003) suggests there may be differential or even conflicting attitudes regarding concern about entities that collect personal data and concern about certain practices themselves. Thus, for a more nuanced understanding of the role of concern, we account for each of these dimensions. This survey modified Westin's items into two kinds of concern on a 6-point scale that asked users' agreement over the statement assessing anxiety level, anchored with *strongly agree* and *strongly disagree*. The first two items asked the respondents to rate the intensity of surveillance concern over different entities: (1) business ($M = 3.34$, $SD = 1.22$) and (2) government ($M = 3.00$, $SD = 1.20$). In the two additional items, respondents were asked to rate the intensity of the concern over intentions behind different information surveillance aspects: (1) data collection ($M = 2.74$, $SD = 1.35$) and (2) appropriation ($M = 3.57$, $SD = 1.20$).

[1] In this case, we are primarily interested in testing different levels of knowledge, i.e., the extent to which effects of knowledge will hold in a weak concern but not in another. Our theoretical interest in the psychological interaction lends itself to this model specification as there is a unexpectedly weak or inconsistent relation between a predictor (i.e., concern) and a criterion variable (i.e., protective behavior) (Barren & Kenny, 1986), rather than a mediating model that is apt for testing causalities in a temporal sequence.

Author's personal copy

In order to examine the dimensions of privacy concern, the items were factor analyzed and extracted into two latent variables. The simple unconstrained and unrotated solution[2] confirmed an emergence of a two factor solution: (1) worry over entities (two items of business and government) and (2) worry over information aspects (two items of collection and appropriation), with a principal component matrix of .80 (eigenvalue of 1.92, explained variance of 48.07%, Cronbach alpha = .63). For the creation of the two factors used in regression models, the scales of concern items were reversed so that positive scores indicate more intense affective concerns. The correlation between the two factors is .320, $p < 0.01$, indicating the two concern factors are also significantly connected.

5.2.3. Reward

Reward was operationalized by the level of likelihood to trade off different types of personal data for financial gain or access to favorable content. The question was modified from Turow (2003), with more emphasis on specific scenarios in which individuals were asked, anchored on *not at all likely* and *very likely*, to imagine the likelihood of divulging data in their rational assessment. The survey participants responded to the following inquiry:

> Imagine you come across a website and it asks you to provide personal information about yourself in exchange of a free gift or access to its content you find interesting. How likely is it that you will provide each of the following types of personal information for a free gift or access to the content?

Then, each item was listed to rate the likelihood on a 6-point scale. Nine data items were drawn from Ackerman, Cranor, and Reagle (1999), Acquisti and Grosslags (2005), Culnan (1995), and Ribak and Turow (2003). The Reward Index ($M = 20.31$, $SD = 9.52$, Cronbach alpha = .86) was created as a composite index of the nine items to capture the extent to which users perceive the likelihood of divulging data for reward or benefit at hand.

5.2.4. Information protection behavior

One of the main purposes in this study was to identify information control behavior as currently performed in daily routine. Information control was operationalized as user behavior in strategizing information release – that is, to opt out or not. The central interest here was to capture how users systematically manage/control personal data and its flow (that can be associated with one's identity). Note that personal information control is "multifaceted" in nature, requiring the combination of social and technical skills as intertwined in Internet uses (Turkle, 1995). This study elaborated pre-existing survey items into (1) social privacy control and (2) technical privacy control dimensions (Marx, 2003).

Each survey item was modified from the extant literature (Acquisti, 2004; Pew Internet, 2005; LaRose & Rifon, 2007; Metzger, 2007; Turow, 2003; Turow et al., 2005). Informed by the pre-established items, the survey aimed to establish the criterion validity of each item. Questions on a six-point scale, ranging from *never* to *very often*, asked: (1) the types of information strategies adopted and (2) the intensity, as indicated in frequency, of such strategies. The composite index (summation of items) was created to construct a continuous scale in each dimension ($M = 24.81$, $SD = 9.18$, Cronbach alpha = .80 for social dimension; $M = 13.12$, $SD = 5.18$, Cronbach alpha = .70 for technical dimension). Table 1 describes all question items.

[2] We also ran Varimax rotated factor analysis and detected the same pattern of an emergence of a two factor solution, with no difference between two analyses in identifying the distinctive concerns of information aspects and entities.

5.2.5. Covariates

The analysis included two levels of covariates. For the first level, five items of demographic characteristics, income (19 categories, $M = 12.70$, $SD = 3.59$), age (7 categories, $M = 3.69$, $SD = 1.65$, gender (high for female), race (high for white), and education (4 categories, $M = 2.97$, $SD = 0.93$) were used. Prior studies consistently documented the role of socio-economic status in maintaining different levels of divide in user behavior. For the second level, two items measured online experiences as these were related to differentiated uses of the Internet (Boyd & Hargittai, 2010; Hargittai, 2004): (1) the minute of Web browsing per week ($M = 297.51$, $SD = 303.54$) (logged) and (2) the number of years in Internet use ($M = 11.06$, $SD = 4.41$). According to Hargittai (2004), the freedom to be able to use the Internet anytime, anywhere, and with any purpose is also one of the most significant single predictors for online skills, as those with more access are likely to be more sophisticated in Web uses. An item was added to observe the number of Internet access points ($M = 2.32$, $SD = 1.31$).[3]

5.3. Analysis

To carry out the analyses, this study constructed a total of twelve two-way and three-way interaction terms. The variables were standardized prior to the formation of the interaction terms to reduce potential problems with multi-collinearity (Campbell & Kwak, 2010). Each level of explanatory variables was entered in the order of covariates (socio demographics, Internet use, and reward), affect and cognition in hierarchical regression analyses. Analyses were run to test the hypotheses pertaining to each of the interactions between concern and knowledge. Likewise, separate analyses were conducted for three-way interactions, after controlling all prior blocks that included the reward variable and its two-way interactions.

6. Results

Table 2 depicts findings from hierarchical regression models of direct associations for main variables in each dimension of privacy protective behaviors. As shown in Table 2, control variables, as a block, accounted for a significant amount of variance in the criterion variables (R^2 is around 15%).[4] After controlling the prior block, consistent and positive associations for knowledge in privacy protection behaviors were found (for social, $\beta = .35$, $p < .001$; $\beta = .29$, $p < .001$; for technical, $\beta = .27$, $p < .001$; $\beta = .20$, $p < .001$). In the affective level, the effects of entity and information concern on technical-dimension protection behavior were marginally negative ($\beta = -.08$, $p < .10$; $\beta = -.09$, $p < .01$). For social-dimension protection behavior, however, no direct relationship for concern was found. The associations between reward and behavior were negative, although they were not found significant.

Findings concerning H1 are presented in Table 3. H1 posited two alternative hypotheses about the moderating effect of knowledge on concern. Overall patterns of the results lend support for H1a – that concern is more strongly associated with protective behavior among those with higher levels of knowledge. Put differently, privacy protection tends to be the highest for those with increased knowledge and a high level of concern. Yet this pattern was found only for the technical-dimension of protection, where the

[3] Autonomy is measured in terms of the number of online access locations individual users have, including laptops, mobile capable online access, etc.

[4] Tech access, yearly experience, and daily uses are strong predictors for different levels of privacy protection. Further, age remains a significant predictor, raising the concern that social divide, independent of knowledge and anxiety, hinders meaningful protection of personal data.

Author's personal copy

Table 1
Survey measures.

		M	*SD*
1.1. Data collection risk			
Companies today have the ability to place an online advertisement that targets you based on information collected on your web-browsing behavior		0.75	0.43
A company can tell you that you have opened an email even if you do not respond		0.57	0.49
When you go to a web site, it can collect information about you even if you do not register		0.65	0.47
Popular search engine sites, such as Google, track the sites you come from and go to		0.66	0.47
E-commerce sites, such as Amazon or Netflix, may exchange your personal information with law enforcement and credit bureau		0.45	0.49
What a computer user clicks while online surfing can be recorded as a trail		0.72	0.44
Most online merchants monitor and record your browsing in their sites		0.68	0.46
When a web site has a privacy policy, it means the site will not share your information with other websites or companies		0.25	0.43
1.2. Regulatory protection			
Government policy restricts how long websites can keep the information they gather about you		0.20	0.40
It is legal for an online store to charge different people different prices at the same time of day		0.22	0.41
A website is legally allowed to share information about you with affiliates without telling you the names of the affiliates		0.40	0.49
By law e-commerce sites, such as Amazon, are required to give you the opportunity to see the information they gather about you		0.14	0.35
Privacy laws require website policies to have easy to understand rules and the same format		0.20	0.40
US government agencies can collect information about you online without your knowledge and consent		0.56	0.49
When I give personal information to an online banking site such as citibank.com, privacy laws say the site has no right to share that information, even with companies it owns		0.22	0.41
1.3. Social privacy control			
Avoidance	Stopped visiting particular web sites because you fear they might deposit unwanted program on your computers	3.21	1.85
Hiding	Given false or inaccurate email address or fake name to websites because of the privacy concern	2.54	1.73
Withdrawal 1	Decided not to make an online purchase because you were unsure of how information would be used	3.42	1.72
Withdrawal 2	Chose not to register on a website because it asked you for personal information to get into the site	4.28	1.63
Complain	Complained to a consumer or government agency about marketing practices of particular websites	1.50	1.07
Rectify 1	Asked a website to remove your name and address from any lists used for marketing purpose	3.51	1.82
Rectify 2	Asked not to share your personal information with other companies	3.58	1.97
Multiple accounts	Used an email address that is not your main address, in order to avoid giving a website real information about yourself	2.89	1.97
1.4. Technical privacy control			
Clearing history	Cleared your web browser history	3.49	1.81
Clearing history	Used filters to block or manage unwanted email	4.56	1.90
Erasing cookies	Erased some or all of the cookies on your computer	3.68	1.90
Using PET	Used software that hides your computer's identity from websites you visit	1.41	1.48
1.5. Affective concern			
Information	When websites, such as Google or Amazon, collect information about me, they do so to provide me with benefits	2.74	1.35
Anxiety	I trust websites not to share information about me with other sites when they say they won't	3.57	1.20
Entity	Most online businesses handle the personal information they collect about consumers in a proper and confidential way	3.34	1.22
Anxiety	Government provides a reasonable level of privacy protection for citizen today	3.00	1.20
1.6. Reward			
Nine different personal data to trade off for convenience are as follows: email address; full name; political orientation; purchase habits; financial record, medical history, type of computer you use; sexual orientation; favorite snack		20.31	9.52

interactions between information concern and both knowledge measures were significant ($\beta = .08$, $p < .05$; $\beta = .09$, $p < .05$).

RQ1 examined the three-way interactions among concern, knowledge, and reward-seeking in predicting privacy protection online. The three-way interaction terms analyzed in Table 4 attempt to understand the function of reward-seeking, with the roles of concern and knowledge simultaneously considered. After controlling for prior blocks and other two-way interactions,[5] hierarchical regression analyses displayed that both information and entity concerns, knowledge of data collection risk, and reward interacted for the social protection measure ($\beta = .15$, $p < .01$; $\beta = .11$, $p < .05$). In predicting the technical measure of protection, the interactions among both information and entity concerns, knowledge of regulatory protection, and reward were found marginally significant ($\beta = .08$, $p < .10$; $\beta = .08$, $p < .10$); however, the three-way interactions predicting technical protection behavior were not significant when shifting from knowledge of regulatory protection to knowledge of data collection risk.

The significant three-way interactions involving both social and technical protection behaviors indicates that with a high level of reward-seeking, concern tends to be more strongly associated with privacy protection for those with higher levels of knowledge than those with lower levels of knowledge. Looking at the low level of reward-seeking, however, privacy protection behavior is the highest for those with increased knowledge and a low level of concern. The findings display that for those with high-reward seeking, as knowledge serves as a missing link between concern and protective behavior, the gap between high and low knowledge widens. The pattern tends to be reversed for those with low reward-seeking as the gap between high and low knowledge shrinks with increased concern, while knowledge appears to help compensate for a lack of concern.

7. Discussion

This study was primarily interested in the interaction effects of privacy concern, privacy knowledge, and reward in predicting privacy protection online. In leading up to the interactions, we tested the direct associations between protective action and the predictor variables. On a direct level, concern did not play a meaningful role in predicting the social dimension of privacy protection, such as

[5] In regards to the two-way interactions between knowledge and reward, marginal supports were found in tech-related privacy protection behavior (knowledge of data risk × reward, $\beta = -.08$, $p < .10$; knowledge of regulatory protection × reward, $\beta = .12$, $p < .10$). Also, there was a moderate support for the interaction between entity concern and reward in social behavior ($\beta = .09$, $p < .10$).

Author's personal copy

Table 2
Hierarchical regression results.

	Social		Tech	
	β	t Value	β	t Value
Covariates				
Age	−.15	−3.01**	−.15	−3.07**
Gender	−.04	−.99	−.13	−2.62**
Race	−.08	−1.67#	.03	.61
Education	.10	2.02*	.05	1.01
Income	−.07	−1.39	−.03	−.57
Yearly experience	.22	4.47***	.21	4.34***
Daily use (logged)	.16	3.32**	.14	3.00**
Autonomy	.11	2.31*	.16	3.27**
Affective dimension				
Information concern	.01	.39	−.09	−2.11*
Entity concern	.01	.22	−.08	−1.79#
Cognitive dimension				
Knowledge of data collection risk	.35	7.33***	.27	5.71***
Knowledge of regulatory protection	.29	6.17***	.20	4.20***
Reward-seeking	−.01	−.24	−.00	−.19

Notes: 1. The coefficients in affective and cognitive dimensions are the results of separate hierarchical regression models while the variables in prior blocks remain constant. 2. Entries are standardized regression coefficients after controlling for the prior blocks.
# $p < .10$.
* $p < .05$.
** $p < .01$.
*** $p < .001$.

avoiding certain web sites or falsifying information to hide one's identity. In fact, technical measures of protective action, such as clearing history and erasing cookies, were actually predicted by lower levels of information and entity concern, however marginally so. These direct associations, with no apparent effect of concern on social protection, seem to illustrate the privacy paradox, or the observation that concern may not "readily" translate into protective action. Although limitations inherent to cross-sectional data hinder causal claims, we can still expect positive correlations between concern and protective behavior if the former leads to the latter, thus allowing us to rule it out in context of this study.

Switching lenses to cognition, the findings show that knowledge played a much more meaningful role in directly predicting privacy protection online. Both forms of knowledge (i.e., knowledge of data collection risk and of regulatory protection) significantly predicted higher levels of social as well as technical dimensions of privacy protection. As with the case of concern, there are theoretical, if not empirical, grounds for speculating on the direction of influence. Although either causal direction is plausible, it seems more plausible that knowledge leads to protective action when considering the alternative. We acknowledge the possibility that avoiding data sharing and technical maneuvers to prevent it can boost the salience of privacy issues, which could lead to information seeking about the risks and regulations associated with personal data collection. But it seems much more likely that having knowledge about these matters motivates and equips individuals to protect themselves, especially considering the extant theory (Goffman, 1965) and research that has been done in this area that suggests this causal linkage between knowledge and public (in)action Acquisti & Grosslags, 2005; Boyd & Hargittai, 2010; Tai et al., 2007; Turow, 2003; Turow et al., 2005.

Reward-seeking was not related to either avoidance or technological means of privacy protection. This is noteworthy considering it is believed that reward plays an important role in preventing protective action online. Although the associations in our findings were consistently negative, they were not statistically significant.

Table 3
Regression analysis: Concern and knowledge.

	Social		Tech	
	β	t Value	β	t Value
Prior blocks R^2 (%)	27.4		23.8	
Interplay				
Knowledge of data collection risk × information concern	.03	.69	.08	1.96*
Knowledge of data collection risk × entity concern	.00	.16	.01	.23
Knowledge of regulatory protection × information concern	.00	.15	.09	2.06*
Knowledge of regulatory protection × entity concern	.02	.57	.04	.82

Notes: 1. Prior blocks include age, gender, race, education, household income, yearly Internet experience, daily Internet use, autonomy, and all the main variables in Table 1. 2. Entries are standardized regression coefficients after controlling for the prior blocks.
** $p < .01$.
* $p < .05$.

Table 4
Regression analysis: Concern, knowledge, and reward.

	Social		Tech	
	β	t Value	β	t Value
Prior blocks R^2 (%)	28.7		25.9	
Three way interplay				
Knowledge of data collection risk × information concern × reward	.15	3.46**	.03	.70
Knowledge of data collection risk × entity concern × reward	.07	1.64#	.05	1.10
Knowledge of protection × information concern × reward	.11	2.42**	.08	1.68#
Knowledge of regulatory protection × entity concern × reward	.05	1.14	.08	1.82#

Notes: 1. Prior blocks include age, gender, race, education, household income, yearly Internet experience, daily Internet use, autonomy, eight two-way interaction terms, and all the main variables in prior models. 2. Entries are standardized regression coefficients after controlling for the prior blocks.
* $p < .05$.
# $p < .10$.
** $p < .01$.

Author's personal copy

On the surface, the immediate interpretation is that seeking rewards in exchange for personal data does not play a meaningful role in the extent to which users take steps to protect their privacy. However, as the interaction effects involving reward show, this is not necessarily the case. As we discuss below, levels of privacy protection differed notably when reward was included as a moderating variable, highlighting an important contribution of this study – that the relationships between variables involved in the privacy paradox are complex and interactive. This is especially evident in the findings for the three-way interaction effects.

7.1. Interactive relationships

Results for the two-way interactions revealed some significant moderating effects between knowledge and concern in predicting technical privacy protection. Fig. 2 shows a coherent pattern when plotting the interactions. In each case, privacy protection behavior is the highest for those with increased knowledge and high levels of concern. We hesitate to make too much of these two-way interactions because only technical dimensions approach significance and, as Fig. 1 illustrates, there are only subtle changes in privacy protection levels that can be explained by the interaction between knowledge and concern. Here we see the declining trend for those with higher concern is lessened by the moderating effect of high regulatory protection knowledge. That is, those who know more about regulations that restrict the appropriation of personal data become less passive about their own protection when they are also concerned about surveillance practices. Here, small effect sizes qualify the extent to which we consider this a strong pattern, but it and the others in the two-way interactions provide support (albeit only moderate) for the possibility that knowledge may help mitigate barriers to protecting personal data online.

These observations, combined with the significant direct associations between knowledge and protection, suggest that knowledge is an important piece of the privacy paradox puzzle. That is, knowledge about data risks and regulations seem to help mitigate the tendency to be passive about protecting personal information online, which raises important policy implications. Many of the existing industry practices to inform users, such as policy statements and program seals, do little to actually enhance understanding of the implications of sharing personal data, nor do they sufficiently motivate protective behavior. That is, more robust prompts and sources of knowledge are needed to equip users with the information and motivation needed to protect themselves online. This recommendation is in accordance with Turow (2003) and Turow et al. (2005), who argue that current FTC guidelines and voluntary industrial programs do not go far enough in protecting users. Enhanced privacy statements are needed to more clearly inform users. Furthermore, these statements should be context-dependent with regard to safety resources available to the user, should they be unaware of protection measures at their disposal (Park, 2011a, 2011b).

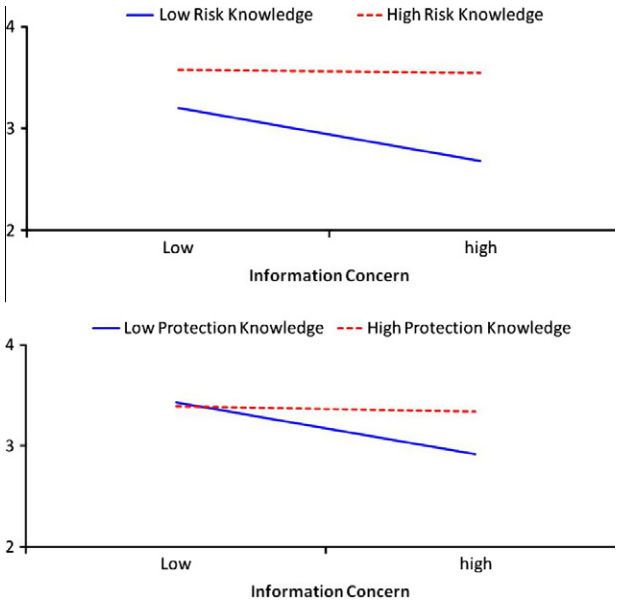

Fig. 2. Predicting privacy protection with knowledge and concern: Technical dimension.

7.2. Three-way interactions

Findings for the three-way interaction effects reveal more notable and divergent trends for privacy protection online. When reward is included as an additional moderator, differential patterns emerge in the extent to which one engages in social as well as technological steps toward protecting their personal information online. First looking at the social behaviors, we see the interactive patterns for knowledge and concern tend to be reversed across the low and high reward-seeking levels (see Fig. 3). That is, the slopes for privacy protection levels tend to either decrease or remain fairly flat for those with high knowledge in the low reward-seeking (left panels of the figures), whereas they tend to rise for those with high knowledge in the high reward-seeking (right panels). Even though reward-seeking was not directly related to social privacy protection practices, it does appear to play an important role as a moderator with the affective and cognitive dimensions. In other words, individuals are noticeably more likely to protect their privacy online through social control when reward-seeking is high and both knowledge and concern are high. These patterns, considered with those for the direct associations, suggest that the role of reward-seeking is heightened, if not activated, by interplay with the affective and cognitive dimensions.

Patterns for the three-way interactions involving technological means of privacy protection are similar for the high reward group (Fig. 4) in that they also consistently reflect increasing levels of protective behavior with increased levels of knowledge. What is interesting about the findings is that the left-hand panels depicting low reward-seeking show declining trends for those with high knowledge, which appears more manifest than the case for social control. It is possible that knowledge of privacy protection regulations combined with an unwillingness to exchange personal data for a reward contributes to less of a perceived need to take actions such as deleting cookies and erasing browsing history, yet at the same time this lack of protective action may feed into increased concern. Assuming for a moment that this is indeed the case, it paints an even more complex picture of the privacy paradox – that low reward-seeking, in the presence of knowledge of regulatory safeguards, may decrease certain (i.e., technological) protective actions more strongly, while (paradoxically) this lack of action heightens concern among users. While theoretically plausible, this interpretation is speculative, and future research is needed to better untangle the interplay and causal flow of these relationships.

Collectively, these findings suggest that the intersections between knowledge, reward, and concern can play out differently, depending on the levels of each. Reward-seeking emerged as an especially important factor in shaping the likelihood to protect one's personal information online; however, this role only appears in concert with differing levels of knowledge and concern. The increasing levels of protective behavior for those with high knowledge in all of the high reward conditions supports those concerned about the use of enticement in getting users to share their personal

Author's personal copy

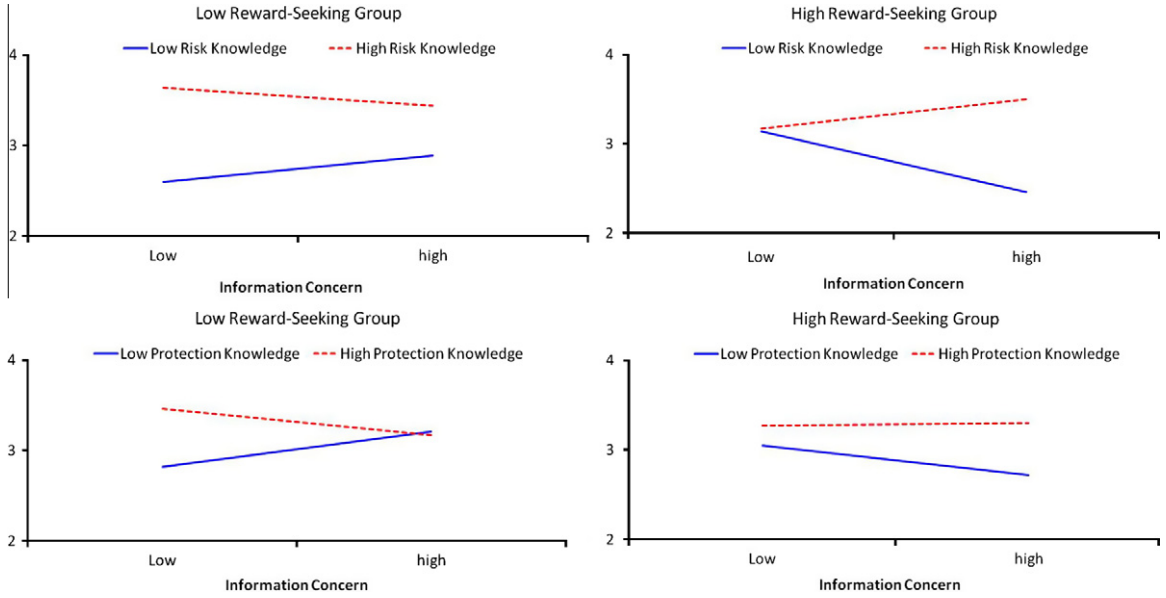

Fig. 3. Three way interactions for privacy protection: Social dimension.

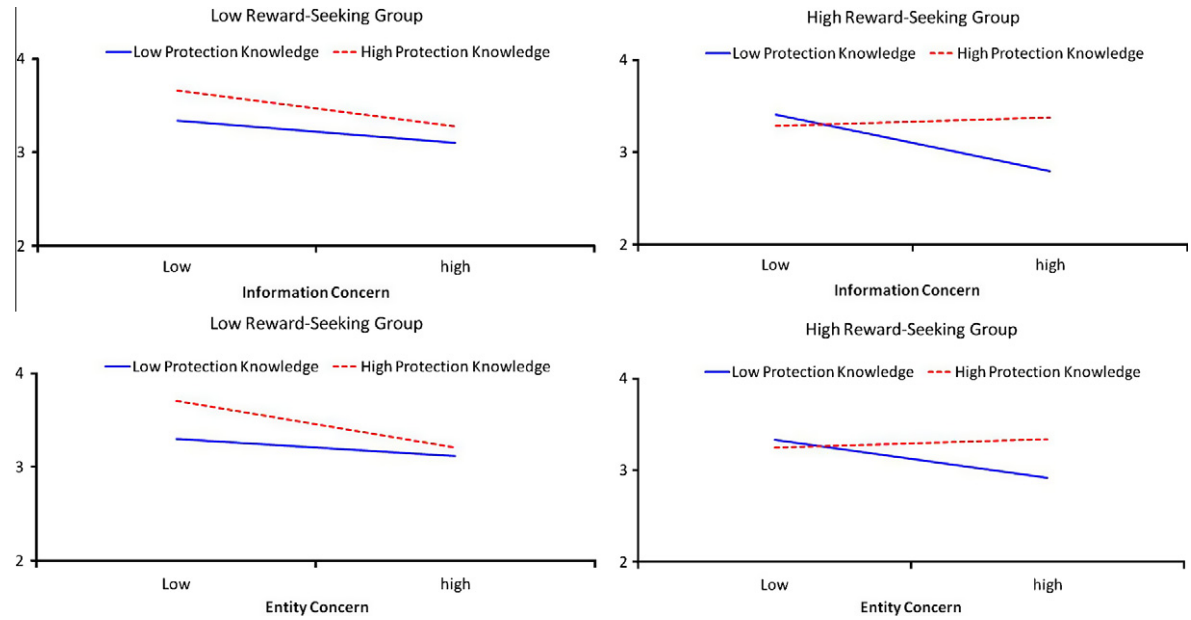

Fig. 4. Three way interactions for privacy protection: Technical dimension.

data (Tai et al., 2007; Turow & Hennessy, 2007; Turow, 2003). In fact, one of the most important insights in this study's findings is that knowledge widens the behavioral gap for those with high levels of concern and this gap appears to be exacerbated by high reward-seeking. Considering the general lack of knowledge about privacy protection and the ineffectiveness of current industry practices in correcting this (Park, 2011b; Turow et al., 2005), policies may be in order to curb the (apparently compelling) promise of rewards in exchange for personal data. In this regard, a primary contribution of this study is to uncover the role of reward-seeking in reversing the trends for social and technical privacy control by taking an interactive approach to the analysis. Indeed, the puzzle of the privacy paradox is complicated, and the underlying mechanisms are not always evident through bivariate correlations, as seen here in the case of reward.

8. Conclusions

In sum, one broad theoretical implication of our findings is that information behavior is a delicate process, arising from intimate interplay with affect and cognition, of which the highly functional dynamics are further compromised in such rationale as reward-seeking. Our contribution is to advance this critical insight in privacy protective behavior in multidimensional measures. Evident is the function of knowledge where the interactive effects are subtle and depend on levels of concern and, particularly, reward-seeking. As this interplay helps us understand privacy protective behavior in virtual environments, the insights may be adaptable to examining other behaviors in mobile telephony, video game uses, or health-related behaviors. Future challenges remain in applying this understanding beyond online information behavior.

Author's personal copy

Moreover, experimental stimulus that generates cognition-knowledge, affect-concern, and reward-seeking in a more explicitly causal context will advance this study's findings in laboratory replication.

References

Ackerman, M., Cranor, L., & Reagle, J. (1999). *Beyond concern: Understanding net users' attitudes about online privacy. AT&T labs-research technical report.*

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the ACM electronic commerce conference (EC04)* (pp. 21–29).

Acquisti, A., & Grosslags, J. (2005). Privacy and rationality in decision making. *IEEE Security and Privacy, 3*(1), 26–33.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*, 179–211.

Barren, R., & Kenny, D. (1986). The moderator–mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of Personality and Social Psychology, 51*(6), 1173–1182.

Boyd, D., & Hargittai, E. (2010). Facebook privacy settings: Who cares? *First Monday, 15*(8).

Campbell, S., & Kwak, N. (2010). Mobile communication and civic life: Linking patterns of use to civic and political engagement. *Journal of Communication, 60*(3), 536–555.

Chen, K., & Rea, A. (2004). Protecting personal information online: A survey of user privacy concerns and control techniques. *The Journal of Computer Information Systems, 44*(4), 85–92.

Culnan, M. (1995). Consumer awareness of name removal procedures: Implications for direct marketing. *Journal of Direct Marketing, 9*(Spring), 10–19.

Dietrichson, A. (2001). *Digital literacy: How to measure browsing behavior*. PhD dissertation, Columbia University, New York.

Dommeyer, C. J., & Gross, B. (2003). Consumer knowledge, awareness, and use of privacy protection strategies. *Journal of Interactive Marketing, 17*(2), 34–51.

Downs, A. (1957). An economic theory of political action in a democracy. *The Journal of Political Economy, 65*(2), 135–150.

Earp, J., & Baumer, D. (2003). Innovative Web use to learn about consumer behavior and online privacy. *Communications of the ACM, 46*(4), 81–83.

Eveland, W., Hayes, A., Shah, D., & Kwak, N. (2005). Understanding the relationship between communication and political knowledge: A model-comparison approach using panel data. *Political Communication, 22*(4), 423–446.

Goffman, E. (1965). *The presentation of self in everyday life*. University of Edinburgh Social Sciences Research Centre.

Goldman, E. (2003). The internet privacy fallacy. *Computer and Internet Lawyer, 20*(January), 20.

Hargittai, E. (2004). Internet access and use in context. *New Media and Society, 6*(1), 137–143.

Hargittai, E. (2008). The role of expertise in navigating links of influence. In J. Turow & L. Tsui (Eds.), *Hyperlinked society* (pp. 85–103). Ann Arbor, MI: The University of Michigan Press.

Just, M., Crigler, A., & Neuman, R. (1998). Cognitive and affective dimensions of political thinking. In A. Crigler (Ed.), *The psychology of political communication* (pp. 133–148). Ann Arbor, MI: The University of Michigan Press.

Khalifa, M., & Limayem, M. (2003). Drivers of internet shopping. *Communications of the ACM, 46*(12), 233–239.

Kumaraguru, P., & Cranor, L. (2005). *Privacy indexes: A survey of Westin's studies, Institute for Software Research International, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, technical report CMU-ISRI-5-138, December 2005*.

LaRose, R., & Rifon, N. (2007). Promoting i-Safety: Effects of privacy seals on risk assessment and online privacy behavior. *The Journal of Consumer Affairs, 41*(1), 127–149.

MacLeod, C., & Mathews, A. (1988). Anxiety and allocation of attention to threat. *Quarterly Journal of Experimental Psychology: Human Experimental Psychology, 38*, 659–670.

Marcus, G., Neuman, W., & Mackuen, M. (2000). *Affective intelligence and political judgment*. Chicago, IL: University of Chicago Press.

Marcus, G., Neuman, W., & Mackuen, M. (2008). Measuring subjective emotional responses: Contrasting two approaches to measurement. In *The International Society of Political Psychology annual scientific meetings, Sciences Po, Paris, July 2008*.

Marx, G. (2003). A tack in the shoe: Neutralizing and resisting the new surveillance. *Journal of Social Issues, 59*(2), 369–390.

Metzger, M. (2007). Communication privacy management in electronic commerce. *Journal of Computer-Mediated Communication, 12*(2).

Neuman, W. R. (1991). *The future of mass audience*. Cambridge, UK: Cambridge University Press.

Park, Y. J. (2008). Privacy regime, culture, and user practices in the cyber-marketplaces. *Info: Journal of Policy, Regulations, and Telecommunications, 10*(2), 52–74.

Park, Y. J. (2011a). Provision of Internet privacy and market conditions: An empirical analysis. *Telecommunications Policy, 35*(7), 650–662.

Park, . Y. J. (2011b). Market philosophy and information privacy. *Javnost – The Public, 18*(2), 87–100.

Pastore, M. (1999). *Consumers will provide information for personalization. Marketing news and expert advice*. <http://www.clickz.com/clickz/stats/1717721/consumers-will-provide-information-personalization> Accessed 09.08.11.

Pew Internet (2005). *Spyware: The threat of unwanted software programs is changing the way people use the Internet*.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and willingness to provide personal information. *Journal of Public Policy and Marketing, 19*(1), 27–41.

Ribak, R., & Turow, J. (2003). Internet power and social context: A globalization approach to Web privacy concerns. *Journal of Broadcasting and Electronic Media, 47*(3), 328–349.

Tai, J., Egelman, S., Cranor, L., & Acqusti, A. (2007). The effect of online privacy information on purchasing behavior: An experimental study. *Proceedings of International Conference of Information System (ICIS)*, 1–33.

Turkle, S. (1995). *Life on the screen: Identity in the age of the Internet*. New York: Simon & Schuster.

Turow, J. (2003). *Americans and online privacy: The system is broken. Report of the Annenberg Public Policy Center.*

Turow, J., Feldman, L., & Meltzer, K. (2005). *Open to exploitation: American shoppers online and offline. Report of the Annenberg Public Policy Center.*

Turow, J., & Hennessy, M. (2007). Internet privacy and institutional trust: Insights from a national survey. *New Media and Society, 9*(2), 300–318.

Uslaner, E. (2004). Trust, civic engagement, and the Internet. *Political Communication, 21*, 223–242.

Westin, A. (1998). *Ecommerce and privacy: What net users want. Tech. report for Privacy and American Business and PricewaterhouseCoopers.*

White, T. B. (2004). Consumer disclosure and disclosure avoidance: A motivational framework. *Journal of Consumer Psychology, 14*(1 and 2), 41–51.