Unlocking the Privacy Paradox: Do Cognitive Heuristics Hold the Key?

Abstract

Even though users have become increasingly concerned about their privacy online, they continue to disclose deeply personal information in a number of online venues, including e-commerce portals and social networking sites. Scholars have tried to explain this inconsistency between attitudes and behavior by suggesting that online users consciously weigh the trade-off between the costs and benefits of online information disclosure. We argue that online user behaviors are not always rational, but may occur due to expedient decision-making in the heat of the moment. Such decisions are based on cognitive heuristics (i.e., rules of thumb) rather than on a careful analysis of each transaction. Based on this premise, we seek to identify the specific triggers for disclosure of private information online. In the experiment reported here, we explore the operation of two specific heuristics—benefit and fuzzy boundary—influencing privacy-related attitudes and behaviors. Theoretical and design implications are discussed.

Author Keywords

Online privacy; information disclosure; personalization.

ACM Classification Keywords

H.5.2 [Information interfaces and presentation]: User Interfaces; J.4. Social and Behavioral Sciences.
**Introduction**

Even though online users are quite wary of privacy infringement on the Internet [e.g., 9,10,11], they continue to share private aspects of their lives on social networking sites (SNS), provide personally identifying information for creating profiles on shopping sites, and use online personalized services that track and analyze their behaviors. This tendency for privacy-compromising online behavior in the face of privacy concerns is known as “privacy paradox” [e.g., 1].

In general, scholars have been trying to understand online privacy disclosure behaviors based on the assumption of a rational decision-making approach on the part of users, in keeping with communication privacy management (CPM) theory [12]. According to CPM, users develop rules of information disclosure by evaluating the related risks and benefits in order to effectively manage individual privacy. Researchers have proposed that certain individual perceptual factors, such as the level of one’s privacy concerns, degree of perceived risk in a transaction, and trust toward the vendor, are key determinants of online privacy-disclosure behaviors [3,9,11]. Qualitative interviews with blog users reveal that they frequently exclude specific groups of people from reading their social media postings [6]. A survey suggested a conscious calculation of the trade-off between concern for privacy and perceived value of personalization [3]. Yet another study posited that privacy risk influences disclosure intention whereas trust leads to actual disclosure behavior, thereby causing the privacy paradox [11].

While this rational-user perspective appears reasonable in the abstract, it is unlikely to reflect the reality of our online interactions and transactions. Given the time-sensitive nature of much of our online activities, we probably are less deliberate and more impulsive in our actions. Moreover, the complexity of privacy settings may serve to inhibit our adherence to the privacy-protection ideals that users self-report in surveys, thereby explaining the seemingly paradoxical behaviors.

Over 30 years of research in social cognition has shown that humans are “cognitive misers” [5] who make decisions that maximize efficiency at the cost of thoroughness. They do so based on cues which suggest “cognitive heuristics” (or mental short-cuts) to desired outcomes by obviating the need for effortful decision-making. For example, the “length equals strength” heuristic would suggest to users that a long message is a strong message, leading them to judge the content of the message as strong even without reading it. In the online context, studies have shown that credibility is often determined by surface level aspects of site design [13]. According to the MAIN Model, interface cues conveying the system’s affordances related to modality, agency, interactivity, and navigability can instantaneously trigger heuristics about the nature of the underlying content [13].

The process outlined by the MAIN Model and the privacy concepts introduced by CPM (like “fuzzy boundary” and “benefit”) lead us to expect that certain interface cues may trigger specific privacy-related heuristics that determine individuals’ online information disclosure behaviors. For instance, interface cues in online personalization systems may trigger privacy-related heuristics that are either negative (e.g., “personalization means my information may be shared with third parties, therefore it may be at risk of leakage”- i.e., fuzzy boundary heuristic) or positive...
(e.g., “my personal information will be used to provide services specifically tailored for me”- i.e., benefit heuristic). In order to ascertain which type of heuristic is triggered when a site offers personalization in exchange for personally identifying information, we first manipulate accessibility of one of the privacy heuristics (i.e., fuzzy boundary, benefit heuristic, or control). After this “priming” phase [2], participants will be assigned an ostensibly unrelated task with a website that either features personalization cues or no such cues, so that we can examine whether the previously primed privacy heuristic will be triggered by the personalization cues, and consequently determine participants’ disclosure behaviors (assessed in the form of a consumer survey requesting personal information).

Based on a pure priming effect, we expect the primed heuristic to play a role in disclosure behaviors, such that those primed with benefits of personalization are more likely to disclose than those primed with the notion of fuzzy boundary (H1). MAIN model would predict this effect to be stronger for those interacting with a personalized site than a non-personalized site (H2; see Figure 1). However, if online users are systematically analyzing privacy risks and benefits when they interact with the interface, as posited by CPM theory, then online disclosure behaviors will not be influenced by the primed heuristics (H3, the competing hypothesis for H1 and H2).

**Study Design**

To test the hypotheses, the current study employed a 3 (benefit heuristic priming vs. fuzzy boundary heuristic priming vs. control) × 2 (personalized website vs. generic website) full factorial between-subjects experimental design (N = 99).

**Stimulus and Manipulation**

Heuristic priming was manipulated through three similar-length video clips (2’15”). Specifically, the benefit heuristic was primed by showing a futuristic vision of personalization services, whereby various systems work together to make life very convenient for users (http://www.youtube.com/watch?v=JSgSiK8-RJc).

In contrast, the fuzzy boundary heuristic was primed with a video depicting a pizza delivery order that is personalized based on the caller’s personal information, including his health conditions and purchasing habits, without his consent (http://www.youtube.com/watch?v=RvYFs9nXTko). For the control condition, a video clip about the formation of hurricanes (http://www.youtube.com/watch?v=0JZcZE7DwyA) was used.

To manipulate personalization, two fictitious shopping websites were created. The first website, called “CoziStore,” was common to all participants. The second website, called “Moo,” was created to have two different versions, a personalized and a generic version. A greeting with participant’s first name, location-based advertisements, display of the specific products that they previously browsed (when in CoziStore), and personalized product recommendations distinguished the personalized version of the Moo site (see Figure 2) from the generic version of the same website.

**Procedure**

Participants were told that they would take part in two separate studies: The first study was to explore audience perceptions of an online video clip, conducted by the College of Communications. Another one was to investigate usability of two online shopping websites, conducted by the College of Information Sciences and Technology. The real purpose of the first study was to

---

**Figure 1.** Hypothesized interaction effect between heuristic priming and types of website on privacy disclosure

**Figure 2.** Personalized version of Moo site
prime one of the privacy-related heuristics with a stimulus video and that of the second study was to provide personalization cues in the treatment condition in order to investigate whether these cues would trigger the heuristic primed in Study 1.

In study 1, after participants watched the assigned video clip, they were asked to complete a bogus questionnaire about their evaluations of the video. In study 2, participants were asked to evaluate the two different websites, CoziStore and Moo. For the first website, each participant was provided with a list of tasks (e.g., “register on the register page,” “add the item priced at $19.99 to the basket”). They were told that the purpose of the “individually assigned tasks” was to systematically evaluate the usability of the website. (In reality, all participants were provided with the same browsing tasks so that the researchers could create the second website for the personalization condition a priori, as well as control for content variations across study participants). Then, they were asked to freely browse the second website (Moo), either the personalized or the generic version (3 min). Attitudes toward the website and trust toward the website vendor were then assessed. After the second study, participants were requested to complete one final questionnaire that was framed as an online consumer survey conducted by the company for understanding potential customers and offering special promotions. The questionnaire included a list of questions requesting participants’ private information. All questions had a “prefer not to answer” option.

**Measures**

The “consumer survey” items were clustered into 3 categories—personal profile, social relations and family-related information. The number of items answered was used as the disclosure measure for each category (See Table 1). Participants’ attitudes toward websites were measured with 11 items, such as “appealing” and “interesting” [7] (Cronbach’s α = .96). Perceived trust toward the vendor of the second website (Moo) was measured with 5 items [9], including “reliable” and “honest” (Cronbach’s α = .95). As a control variable, power usage (or perceived efficacy and expertise in technology use) was assessed with 12 items [8], such as, “I make good use of most of the features available in any technological device” (Cronbach’s α = .82).

**Table 1.** Private information asked in the consumer survey (privacy disclosure measures)

<table>
<thead>
<tr>
<th>Personal profile</th>
<th>Social relations</th>
<th>Family related</th>
</tr>
</thead>
<tbody>
<tr>
<td>• email address</td>
<td>• # of Facebook friends</td>
<td>• father’s education level</td>
</tr>
<tr>
<td>• cell phone number</td>
<td>• # of Twitter friends</td>
<td>• mother’s education level</td>
</tr>
<tr>
<td>• height</td>
<td></td>
<td>• father’s occupation</td>
</tr>
<tr>
<td>• weight</td>
<td></td>
<td>• mother’s occupation</td>
</tr>
<tr>
<td>• last 4 digits of SSN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• number of credit cards you have</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• sexual orientation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• relationship status</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Attitude, trust and power usage were all measured on a 7-point Likert scale, with 7 being most positive.

**Results**

Analyses of covariance, controlling for power usage, showed significant (or near-significant) main effects for the primed heuristic on all three types of information disclosure—Personal profile: F (2, 92) = 3.39, p < .05; Social relationship: F (2, 92) = 5.27, p < .01; and Family-related: F (2, 92) = 2.72, p = .07. Individuals who were primed with the fuzzy boundary heuristic were less likely to disclose their information than other conditions; in contrast, those who were primed with the benefit heuristic tended to report more information than other conditions. However, the effect of personalization cues on the three types of information disclosure was not significant. An interaction effect on personal profile disclosure approached significance, F (2, 92) = 2.73, p = .07 (See Figure 3), but no interaction effect was found for the other two types of information disclosure. In sum, the proposed effects of heuristics (H1) and moderating effects of personalization (H2) were partially supported, and the competing hypothesis based on CPM (H3) was not supported. When attitude
toward the second website and trust toward the vendor were entered as dependent variables, only personalization cues had a main effect on attitude, $F(1, 92) = 3.26, p = .07$ and trust, $F(1, 92) = 4.62, p < .05$. Results showed that those who interacted with the personalized website responded more positively than those who interacted with the generic website.

**Discussion**

The results suggest that online users’ privacy disclosure behavior is more likely to be heuristic rather than systematic. However, more experimentation is needed before we can be dispositive of these findings. The study results also suggested an interaction between the heuristic primed and personalization cues on users’ personal profile information disclosure behavior. However, the direction of the effect did not support our hypotheses. In the generic website condition, the level of disclosure varied as a function of the heuristic primed by the video, such that participants in the control condition tended to reveal more private information than those in fuzzy boundary and benefit conditions. This result implies that the default tendency among online users is to be relatively careless in protecting private information, with the fuzzy-boundary prime suppressing this tendency. On the other hand, for those interacting with a personalized website, this prime failed to have the intended negative effect; in fact, contrary to our expectation, they revealed more personal information than those in the general website condition (see Figure 3). A possible explanation is that, when the fuzzy boundary heuristic is primed, personalization cues on the interface actually served to clarify how personal information is used by the system and thereby assured users rather than increased their privacy concerns. The absence of any such cue in the generic website condition probably led to uncertainty about how the system would utilize or share the personal information.

Another interesting finding is that, unlike the disclosure behaviors, evaluative measures of the website and the vendor were influenced by the existence of personalization, regardless of the privacy heuristic primed. This result provides a viable explanation for ‘privacy paradox.’ According to attitude theories, such as the theory of planned behavior (TPB), a combination of perceptual factors, such as attitude toward behavior and subjective norms, shapes individual’s behavioral intention [1]. Presumably, systematic evaluation of the website is reflected in attitude and trust measures, with an overall positive disposition toward personalization; therefore, heuristics did not play a role in these perceptions. However, heuristics appear to influence actual disclosure behavior, independent of behavioral intention. Therefore, the self-reports of increased privacy concerns noted in surveys of online users could be a product of systematic processing (as predicted by CPM), but actual privacy behaviors are probably driven by heuristic processing (as predicted by MAIN Model).

Together, the findings of this exploratory study suggest that users in general are positively disposed toward personalization systems and will enter personal information into them unless they are primed with heuristics related to specific privacy violations such as fuzzy boundary. This means interfaces have to convey the intentions and outcomes of affordances to the user, with a view to making certain constructs (like fuzzy boundary or benefit) more accessible than others in the user’s mind. Therefore, the current findings hold UI design implications for privacy-related cues on the
interface, both in terms of assuring users of system security of their personal information and in terms of warning users about revealing sensitive information. Ongoing work in our lab group is devoted to identifying specific interface cues that are capable of triggering heuristics. We are also in the process of enumerating various privacy-related heuristics. The ultimate goal is to build empirical links between specific interface cues and cognitive heuristics, and explore how these links influence credibility of systems as well as privacy-related disclosure behaviors online.

Acknowledgements
The first author was supported in this research by a grant from the World-Class University program (R31-2008-000-10062-0) of the Korean Ministry of Education, Science and Technology, awarded to the Department of Interaction Science, Sungkyunkwan University, Seoul, where he serves as a visiting professor. All other authors were supported by Summer Research Grants awarded by the College of Communications at Penn State University.

References