User Disbelief in Privacy Paradox: Heuristics that Determine Disclosure

Andrew Gambino

Media Effects Research Laboratory
College of Communications
Pennsylvania State University
University Park, PA 16802, USA
aug268@psu.edu

Jinyoung Kim

Media Effects Research Laboratory
College of Communications
Pennsylvania State University
University Park, PA 16802, USA
juk315@psu.edu

S. Shyam Sundar

Media Effects Research Laboratory
College of Communications
Pennsylvania State University
University Park, PA 16802, USA
sss12@psu.edu

Jun Ge

Center for Human-Computer
Interaction
College of Information Sciences
and Technology
Pennsylvania State University,
University Park, PA 16802, USA
jug264@psu.edu

Mary Beth Rosson

Center for Human-Computer
Interaction
College of Information Sciences
and Technology
Pennsylvania State University,
University Park, PA 16802, USA
mrosson@ist.psu.edu

Author Keywords

Privacy; privacy paradox; cognitive heuristics; Internet security; information disclosure

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the Owner/Author. Copyright is held by the owner/author(s).

CHI'16 Extended Abstracts, May 07-12, 2016, San Jose, CA, USA
ACM 978-1-4503-4082-3/16/05.

<http://dx.doi.org/10.1145/2851581.2892413>

Abstract

We conducted a series of in-depth focus groups wherein users provided rationales for their own online privacy behaviors. Our data suggest that individuals often take action with little thought or evaluation, even showing surprise when confronted with their own behaviors. Our analysis yielded a battery of cognitive heuristics, i.e., mental shortcuts / rules of thumb, that users seem to employ when they disclose or withhold information at the spur of the moment. A total of 4 positive heuristics (promoting disclosure) and 4 negative heuristics (inhibiting disclosure) were discovered. An understanding of these heuristics can be valuable for designing interfaces that promote secure and trustworthy computing.

ACM Classification Keywords

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

Introduction

It appears that far too often users are clicking “I agree,” or sharing their personal information, without reflecting on their actions. This notion is neglected by traditional approaches to Internet privacy that assumes a rational, thoughtful user [4, 17]. Given the time-sensitive nature of many online tasks, we are likely to be less deliberate in our actual actions [16]. In fact, the progression of research and results of empirical studies

has led many to believe that a privacy paradox may exist (i.e., individuals betray their privacy attitudes and share more than they admit to sharing) [13].

Behavioral economist Allesandro Acquisti and colleagues [1, 2, 6] found that individuals are prone to non-rational, valuation of their personal information in different settings, often driven by subtle psychological and emotional nudging. They concluded that users often act according to these biases when making privacy-related decisions, based on *bounded rationality*. Further, these nudges can manifest in the form of interface cues. Research on the effects of visual cues has been shown to significantly alter privacy behaviors. For example, Serge Egelman and colleagues [5] demonstrated that an encouraging password meter resulted in stronger user-generated passwords.

In sum, online users' approach to privacy appears to be contextually determined [12, 14], and not always consistent with their explicit ideals. User decision-making in different contexts may be governed by rationales outside the purview of traditional cost-benefit analysis in economic theory. In order to discover these rationales, we conducted a series of focus groups that probed participants' privacy and security behaviors.

Method

A series of semi-structured, focus groups were conducted in the Fall and Winter of 2014-15. In total, eight focus group sessions were conducted, with 41 participants taking part in the focus groups. Three groups consisted of university students; five groups consisted of diverse non-student individuals recruited through an ad in a local newspaper. Our recruitment approach resulted in a very diverse sample, with participants ranging from undergraduates to senior

citizens, including individuals who check their twitter feeds hourly to others who do not own a smart phone.

Procedure

The focus group sessions lasted approximately one hour each. The moderator led each group through a semi-structured set of questions focused on their privacy-related behaviors, and encouraged participants to recount in-depth rationales for behaviors during the discussion. These questions, informed by prior research and deliberation, focused on an array of issues, from broad perceptions (e.g., Do you feel more or less safe sharing your information on your mobile as opposed to your laptop or PC?) and behavioral tendencies (e.g., Have you taken any measures to 'hide' your online activity?) to specific actions (e.g., Have you ever changed the privacy settings of your Facebook profile?). There were both pre-written probes and spontaneous follow-up questions aimed at discerning why a particular behavior occurred. Overall, the questions covered six main topics of interest: general privacy and security, mobile, e-commerce, cloud services, online messaging, and social networking sites. Upon completion of the data collection, the focus group sessions were transcribed and analyzed by the research team. The analysis was inductive and data-driven, grounded in the constant comparison approach [10]. Consistent with this approach, the research team thoroughly read, analyzed (coded), discussed, and reanalyzed the data. This analysis, while not yet complete, has yielded common themes for further discussion and interpretation.

Results

The major finding across all our focus groups was an utter sense of disbelief about their own behaviors.

Positive Heuristics

Heuristics that increase information disclosure behavior

Gatekeeping Heuristic:

When a system has many layers of access, it makes me feel safer

Safety Net Heuristic: I am safe because a third-party (e.g., Visa or PayPal) has me covered

Bubble Heuristic: If I am in a protected network, I am safe

Ephemerality Heuristic: If information is not stored but disappears, then it is safe (to share)

Many participants realized that the grounds for their judgments were less than ideal when probed further. For example, one participant shared: *"I know when I log into banking on my computer, they have the little lock on the web browser and that makes me feel secure...[Follow up: why does that make you feel more secure?] It's supposed to be. It says that network is secure. I guess maybe it's not? maybe [pause] it just kind of makes me feel that sense of security."* For that participant, the lock implied a stronger sense of safety, but when he started to really think about that safety, he concluded that what the lock communicated was trivial. However, he still based his judgment and behavior on this hollow rationale.

When asked about privacy-enhancing behaviors, one participant expressed a mix of trust and distrust in Google services, stating: *"I will use Google for anything! But if it's something that I think is kind of sketchy I will use [Google Chrome's] incognito mode because it makes me feel better. Although, I'm sure that [Google] can still track something."* This individual vacillates in his trust of Google, but feels more confident disclosing information because of the mere possibility of gaining extra protection, despite having no real understanding of the operation of 'incognito mode.' Here, the participant seems to rely on a rule of thumb that a system's extra layers of protection allows him to safely reveal more sensitive information. Overall, these decisions seem to be premised on rather quick, in the moment, non-systematic judgment.

This pattern is in contrast to the concept of a privacy calculus and other theories that suggest a rational user approach in privacy decision making. In the above cases, the privacy attitudes of the user did not change, but the heuristic employed nudged them into more

liberal or conservative information disclosing behavior.. It should be noted that there was never a mention of rules of thumb, or cognitive heuristics, in the sessions. As such, we consider this result truly inductive. What follows is a cataloguing of emergent heuristic themes identified as part of the ongoing analyses of transcripts by the research team.

Positive Heuristics

We have identified four dominant reasons why users would feel comfortable revealing their personal information in an online or mobile context.

Gatekeeping Heuristic

The focus group data revealed that users prefer a system that takes overt steps to protect their information. For example, one participant noted *"I know through my bank specifically they have three different check points [security questions; password and picture match] just to get into my account so that makes me feel, I guess, somewhat safer."* Another participant added *"It's some kind of additional layer to try to protect your information and that makes me feel comfortable."* We call this the *gatekeeping heuristic*, and throughout the sessions it was invoked in discussions of very sensitive data (e.g., financial and health information). However, in some cases, particularly for systems requiring frequent log-ins (e.g., Facebook), gatekeeping steps were often described as annoying or a nuisance.

Safety Net Heuristic

Many participants expressed that their fears were alleviated by third party services and systems such as PayPal, their credit-card company, and even Apple. One participant said, *"I perceive PayPal to be more secure*

although I don't know why, because PayPal has direct access to my bank account and everything else it's just a credit card and so there's another barrier there."

Others were more fully positive in their trust of middle men, *"I just say, 'Oh PayPal' and 'Here let PayPal handle this for me! If they don't use PayPal then I'm going to reconsider my purchase."* This underlying thought also extended to general web browsing, with one participant stating that they ignore browser warnings because *"I'm on a Mac, so I'm not that worried."* These examples suggest a rule of thumb that is premised on users' trust that a third party 'has their back' and will guarantee the safety of their personal information. We term this the *safety net heuristic*, where the trusted third-party makes it safe to disclose information.

Bubble Heuristic

Features such as incognito or private web-browser modes, as well as carrying out transactions on one's home network engendered a sense of safety. One participant shared, *"I never really thought I shouldn't be emailing on my cell phone, but I do feel better if I'm at home and it's my tablet or my cell phone and it's on my wi-fi because it's secure and nobody presumably could easily break into it."* Similarly, another participant shared a willingness to disclose some personal information at home but not over public networks or unknown connections such as at a hotel, adding *"Yea so I just kind of am in my own little box [on my own network]."* Indeed research has shown that users tend to have a strong faith in personal wi-fi networks and private browsing modes despite the presence of actual privacy and security risks [7, 9]. Psychologically, the *bubble heuristic* represents additional security when individuals feel that they are in an online 'enclosure' of

some sort, be it a home network, a virtual private network, or a 'virtual mask' such as what may be provided by incognito mode.

Ephemerality Heuristic

Many participants expressed that they felt more comfortable disclosing information over platforms such as Snapchat because they believed content was not being recorded, that it felt transient. As with other heuristics, people recognized the possible fallacy in that hope, but nonetheless felt more comfortable in the moment. For instance, one participant stated, *"Yea and do I feel that their [Snapchat's servers] secure, because I can make it go away. That gives me a sense of security, but I do know that someone could take a screen capture, which makes it less secure but I don't think about that in the moment."* Again, this participant expressed very quick, in-the-moment thinking that was encouraged by what we have termed the *ephemerality heuristic*. When this heuristic is triggered, users feel they can be more open and share more information because there will be no permanent or shareable record. Simply put, if people think the information disappears, they are more likely to share it.

Taken together, these heuristics encourage information sharing or feelings of safety, and in general the rules of thumb had the potential be triggered by interface cues.

Negative Heuristics

We also discovered heuristics that inhibit sharing of information. We have labeled these as "negative" heuristics, in that they are rules of thumb that lead one to distrust a website or restrict sharing of information.

Negative Heuristics

Heuristics that inhibit information disclosure behavior

Fuzzy-boundary Heuristic: My information may be shared with third-parties, therefore it is unsafe

Intrusiveness Heuristic: If something arrives unsolicited, it is unsafe

Uncertainty Heuristic: If I don't understand the interface or how it works, it is unsafe

Mobility Heuristic: That which you carry around is inherently unsafe

Fuzzy-boundary Heuristic

Several participants expressed an unpleasant sentiment when confronted with cumulative evidence of their own behavior, with many citing Facebook and its use of targeted advertising as triggers. One participant stated “[When I am] On Facebook and those advertisements pop up right on the side, that’s where I feel a little bit of uncertainty – It’s a little creepy.” We have termed this phenomenon the *fuzzy-boundary heuristic*, which refers to distrust because one’s information is being shared with a third party without one’s knowledge or consent. From a heuristic angle, the negative effect may be temporary and fleeting, showing short-term reaction change but no long-term attitude change. However, to avoid these negative associations, data minimization may be a sound strategy that industry firms can adopt to deal with one of the relatively few situations in which users may overtly push back with concerns for their privacy [3].

Intrusiveness Heuristic

The unsolicited arrival of emails, requests, notifications, and advertisements was bothersome to the focus group participants. Such requests may function as a regular reminder that the Internet is inherently unsafe, as one participant noted “I don’t like any [mobile] apps that ask me to share information, my answer is no!” Further, one participant spoke out about their negative reactions in the face of pop-ups from everyday Internet use, “Unsafe is when all of a sudden ads pop up after you’ve even just gone to Staples.com.” The *intrusiveness heuristic*, which refers to distrust when individuals receive unsolicited items, seems to be in play across many Internet devices, applications and services. When invoked, users tend to inhibit their sharing of information, or question the integrity of the system or application making or allowing the request.

Uncertainty Heuristic

Systems and technologies that are new or unfamiliar also raise user concerns about information sharing. For the most part, individuals felt immediate discomfort with the unknown. When asked about his adoption of the iPhone, one participant said “Absolutely [I felt insecure on the iPhone], because it was new to me, there were a lot of things I couldn’t figure out... So I felt fairly naïve about it, I didn’t feel real secure with it in any sense.” Moving beyond devices, another participant showed skepticism for cloud services “I just wonder who or where is this cloud and who’s in charge of it, you know it just seems so unknown and therefore very insecure.” Research has shown that individuals generally feel safer with storage on their own devices than over ‘the cloud’ [8]; uncertainty may well be the underlying reason. In these cases, the rule of thumb at play was the *uncertainty heuristic*, referring to situations where individuals felt unsafe because of their lack of understanding of the device or website.

Mobility Heuristic

When asked why she would not order via her mobile phone on Amazon.com, one participant said “Because I think it’s [mobile] probably less secure than doing it on my PC. I don’t know, a computer seems safer than a mobile phone for me.” A few participants expressed a similar sentiment that was admittedly not based on specific knowledge, “I don’t know why I would feel safer on my desktop, I just do.” In addition to the public nature associated with mobile communications these concerns seem to be specific to use of mobile products. The *mobility heuristic* (i.e., devices that you carry around are unsafe) may have been triggered by network cues, the steal-ability of devices that can be

carried [11], and perhaps the novelty of mobile technology.

In summary, the focus group sessions we conducted lend strong support to the role of a variety of cognitive heuristics that may be active in privacy and security related decisions.

Discussion

Our qualitative data and analysis allow us to make a contribution to the privacy literature by uncovering and classifying a wide range of cognitive heuristics. The identification and analysis of heuristics is a big step in organizing further research on privacy behaviors.

This study finds users premising their decision making on interface-cue triggered cognitive heuristics. Like Sundar and colleagues suggested [14, 16], the results show that cognitive heuristics may serve as an explanation for the privacy paradox. With the identification of user dependence on psychological rules, researchers have an additional explanatory mechanism, armed with evidence that merely asking users about their normative behaviors is not enough to report on actual behaviors. The themes from the focus groups touch on matters of user-psychology, human-computer-interaction, and communication, but focus on the heuristics that may guide the behaviors of users.

This research paper has catalogued a number of cognitive heuristics, and suggested ways that cues may be utilized to trigger the discussed heuristics. It is our hope that the design community can utilize these heuristics to design more secure interfaces and encourage responsible user behavior. The cognitive heuristics mentioned in this paper can each be traced back to a specific interface cue. For example, the fuzzy-

boundary heuristic may be triggered by an advertisement that features private user information. Even the more abstract heuristics, such as the ephemerality heuristic, can be tied to the interface, in this case being the visual 'disappearance' of their information.

Based on discussions in our focus groups, interface cues appear to be quite powerful in triggering heuristics. While experimental data are needed to test the causal effects of cues and the role played by the aforementioned heuristics in privacy decision-making, identification of eight specific heuristics can help the design community to come up with cues, nudges and affordances that can promote more secure and trustworthy computing. In doing so, designers ought to be ethical in their use of these heuristics and avoid tricking users into revealing personal information that may compromise their privacy.

Acknowledgements

This research is supported by the U. S. National Science Foundation (NSF) via Standard Grant No. CNS-1450500.

References

1. Acquisti, A. 2012. Nudging privacy: The behavioral economics of personal information. *IEEE Security & Privacy*, 6, 82-85.
2. Adjerid, I., Acquisti, A., Brandimarte, L., and Loewenstein, G. 2013. Sleights of privacy: Framing, disclosures, and the limits of transparency. *In Proceedings of the Ninth Symposium on Usable Privacy and Security* (Newcastle, UK, July 2013) ACM, 9.

3. Camp, L. J. 2015. Respecting people and respecting privacy. *Communications of the ACM*, 58, 27-28.
4. Culnan, M. J., and Armstrong, P. K. 1999. Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, 10, 104-115.
5. Egelman, S., Sotirakopoulos, A., Muslukhov, I., Beznosov, K., and Herley, C. 2013. Does my password go up to eleven?: the impact of password meters on password selection. In *Proceedings of the 31st SIGCHI Conference on Human Factors in Computing Systems* (Paris, France, April 2013) ACM. 2379-2388.
6. Egelman, S., Tsai, J., Cranor, L. F., and Acquisti, A. 2009. Timing is everything?: the effects of timing and placement of online privacy indicators. In *Proceedings of the 27th SIGCHI Conference on Human Factors in Computing Systems* (Boston, MA, April 2009). ACM. 319-328.
7. Gao, X., Yang, Y., Fu, H., Lindqvist, J., and Wang, Y. 2014. Private browsing: An inquiry on usability and privacy protection. In *Proceedings of the 13th Workshop on Privacy in the Electronic Society* (Scottsdale, AZ, November 2014). ACM. 97-106.
8. Ion, I., Sachdeva, N., Kumaraguru, P., and Čapkun, S. (2011, July). Home is safer than the cloud!: Privacy concerns for consumer cloud storage. In *Proceedings of the Seventh Symposium on Usable Privacy and Security* (Pittsburgh, PA, July 2011) ACM. 13.
9. Klasnja, P., Consolvo, S., Jung, J., Greenstein, B. M., LeGrand, L., Powledge, P., and Wetherall, D. 2009. When I am on wi-fi, I am fearless: Privacy concerns & practices in everyday wi-fi use. In *Proceedings of the 27th SIGCHI Conference on Human Factors in Computing Systems* (Boston, MA, April 2009). ACM. 1993-2002.
10. Krueger, R. A., and Casey, M. A. 2000. *Focus groups: A practical guide for applied research*. Sage Publications, Thousand Oaks, CA.
11. Matthews, T., Pierce, J., and Tang, J. 2009. No smart phone is an island: The impact of places, situations, and other devices on smart phone use. *IBM RJ10452*.
12. Nissenbaum, H. 2009. *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press, Palo Alto, CA.
13. Norberg, P. A., Horne, D. R., and Horne, D. A. 2007. The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, 41, 100-126.
14. Palen, L., and Dourish, P. 2003. Unpacking privacy for a networked world. In *Proceedings of the 21st SIGCHI Conference on Human Factors in Computing Systems* (Ft. Lauderdale, FL, April, 2009). ACM. 129-136.
15. Sundar, S. S. 2008. The MAIN model: A heuristic approach to understanding technology effects on credibility. In *Digital media, youth, and credibility*, M. J. Metzger and A. J. Flanagin Eds, Boston, MA, MIT Press, 73-100.
16. Sundar, S. S., Kang, H., Wu, M., Go, E., and Zhang, B. 2013. Unlocking the privacy paradox: Do cognitive heuristics hold the key? In *CHI'13 Extended Abstracts on Human Factors in Computing Systems* (Paris, France, April 2013). ACM. 811-816.
17. Xu, H., Luo, X. R., Carroll, J. M., and Rosson, M. B. 2011. The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems*, 51, 42-52.