Why Do We Reveal or Withhold Private Information?

Exploring Heuristics and Designing Interface Cues for Secure and Trustworthy Computing

S. Shyam Sundar[1] (sss12@psu.edu), **Mary Beth Rosson**[2] (mrosson@ist.psu.edu), **Jinyoung Kim**[3] (juk315@psu.edu)

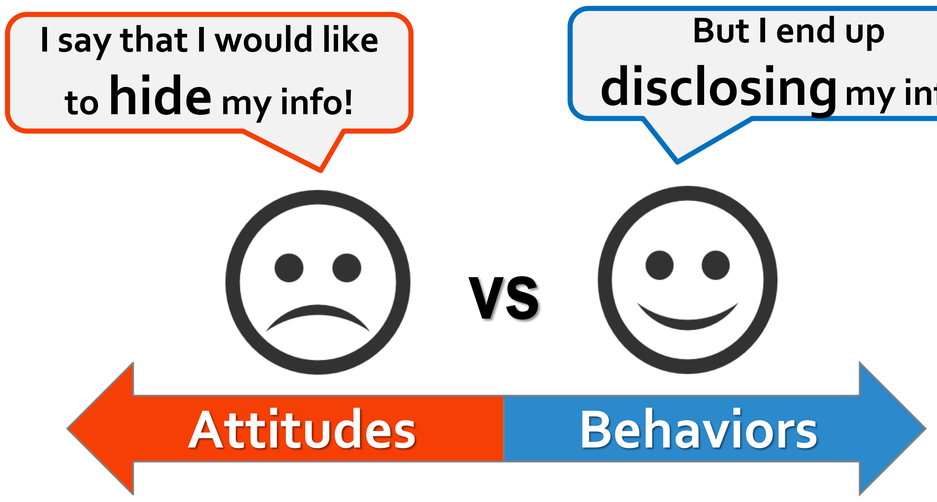
[1] PI, Media Effects Research Lab, College of Communications, Penn State University

[2] Co-PI, College of Information Sciences and Technology, Penn State University

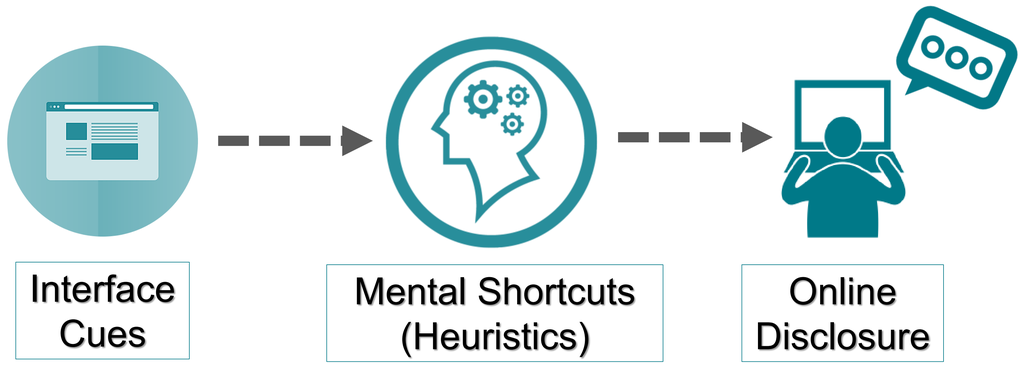
[3] Project Coordinator, Media Effects Research Lab, College of Communications, Penn State University

Background & Our Approach

Privacy Paradox (Norberg, Horne, & Horne, 2007)



The contradiction between users' general privacy concerns and actual disclosure behavior is called "privacy paradox."



Given the cognitively demanding nature of many online transactions, we claim that users' information disclosure behaviors are driven by interface cues in various interaction contexts, which trigger **cognitive heuristics (mental shortcuts)** about the safety/ security of online transactions. An understanding of these heuristics may unlock the privacy paradox.

TRUSTe CERTIFIED PRIVACY → **Authority Heuristic** → **Information Disclosure**

FREE WiFi ZONE → **Publicness Heuristic** → **Information Concealment**

In our project, we aim to discover cognitive heuristics related to users' online security/privacy decision-making, identify the specific triggers of disclosure, design interface cues to evaluate their effects on information disclosure, and provide guidelines to designers and users for secure and trustworthy computing.

Progress

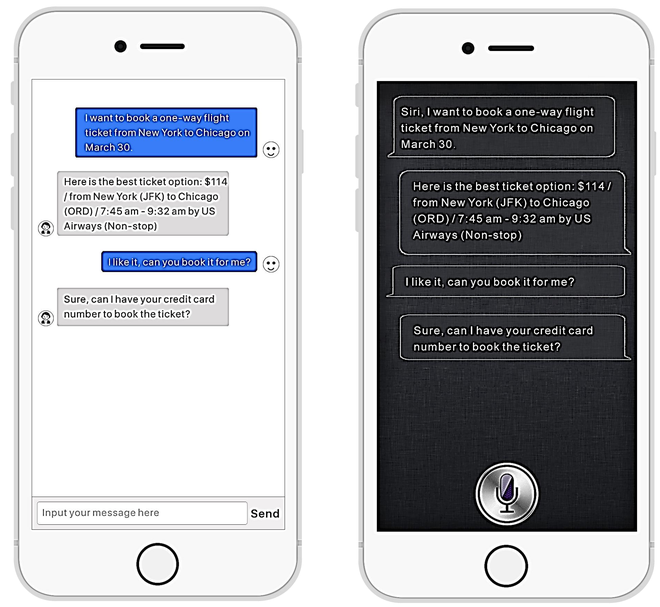
- **Multi-Phased Study**
  - Phase [1]: Focus-group interviews & National survey to identify privacy and security related heuristics employed by users – ***completed***
  - Phase [2]: Design interface cues to trigger heuristics and implement them on mobile/web interfaces, test them through user studies – ***completed***
  - Phase [3]: Online experiment to empirically test the effects of cues on information disclosure and the operation of specific heuristics – ***in progress***

Findings

- All of our studies (**focus-groups, survey, experiments)** show that **online or interface cues** indeed trigger privacy- or security-related heuristics, and their belief in the **heuristics** indeed affect **their decision to reveal or withhold their personal information**

ex) When making a mobile transaction using a credit card number,

- **Machine** interactant → More disclosure
  F (1, 146) = 8.72, $p < .001$, partial η^2 = .07
- **Machine** interactant
  × Greater belief in the machine heuristic
  → More info disclosure
  F (1, 144) = 6.34, $p < .05$, partial η^2 = .05



Examples of Privacy-related Cognitive Heuristics

#1. Sense of Community Heuristic
If I were a part of a community, I would share my information within that community

#2. Bandwagon Heuristic
If majority of other users have revealed information to a site, then I will do the same

#3. Instant Gratification Heuristic
Immediate service is better than delay in satisfaction of my needs

#4. Mobility Heuristic
Mobile devices are inherently unsafe in protecting my information

#5. Self-Presentation Heuristic
The more I reveal, the more I can shape my online persona

#6. Online Security Heuristic
Online is not safe, thus risky to reveal personal information

#7. Fuzzy Boundary Heuristic
Users' online information may be shared, therefore vulnerable

#8. Reciprocity Heuristic
If someone reveals personal information to me, I will do the same in return

#9. Inconsistency Heuristic
Calls for unusual or irrelevant information pose security risk

#10. Transparency Heuristic
If a web site makes its privacy policy transparent, then users' information is safe