Engendering Trust: Privacy Policies and Signatures

Joshua B. Gross, Jessica Sheffield, Alice Anderson, and Nan Yu

The Pennsylvania State University

University Park, PA 16802

jgross@ist.psu.edu, (jessicas, aea145, nxy906)@psu.edu

ABSTRACT

This abstract describes data from an experiment on trust and credibility in political websites. We focus on trust as a crucial mediating variable, and show how the perceived clarity of a privacy policy increases positive reaction to the site and its goals. We also show that providing a signature attached to the privacy policy produces no measurable effect in perception or willingness to offer personal information.

1. INTRODUCTION

In an opportunistic sample[1] of American bank privacy policies (N=10), we found that the mean length was 1,892 words, with a mean Flesch-Kincaid Grade Level of 11.6 and a mean Flesch Reading Ease of 37.1. These data are examples of the horrid state of current privacy policy comprehensibility. While these policies are largely legal documents (not designed for mere mortals to actually read), they can have a significant effect on user perceptions of the credibility of a web site.

Aristotle considered *ethos* (the rhetorical appeal of the speaker) the most important argumentative proof [1]. Trust in the speaker leads to trust in the argument. Our interest was to see if this argument could be operationalized in an online site.

We see trust as an operational aspect of credibility. Fogg [2] describes perceived credibility in web sites as a combination of user's perceptions of the trustworthiness and expertise of the organization. We believe that organizational attitude towards consumers' private information (as expressed in a privacy policy) will influence user perception of credibility. Malhotra *et al.* [4] described information privacy concerns as a person's perception of fair use of their information. As trusting behaviors are a form of risk taking [4], an organization's ability to establish credibility is crucial. The content of the privacy policy is important; Papacharissi & Fernback [5] studied the effectiveness of various aspects of privacy policies for Web portals. They found that language was important to perceptions of credibility and that clarity implied a more sincere policy.

2. STUDY

In order to study trust, credibility, and associated issues, we constructed a weblog for a putative political group, Students for Fair Tuition (SFT), aimed at moderating the increasing tuition cost for a specific university. We then exposed undergraduate students (N=95, each compensated with a small amount of course credit) to the site, allowed them to join a mailing list and/or sign a petition, and asked them to complete two questionnaires. We designed our political issue around the (later validated) assumption that student would generally agree with a mildly political website advocating moderation in tuition increases.

[1] We used the top-ranked consumer bank sites returned from a Google search for "bank".

3. Privacy Policy Perception

After viewing several pages of the weblog, participants were sent to the mailing list/petition page. We included a privacy policy on the same page. The privacy policy was intentionally short (56 words), and designed to be clear (Flesch-Kincaid Grade Level of 8.4, Flesch Reading Ease of 59.6). We did not vary the privacy policy content as an IV, as we felt we would see sufficient distribution in response due to moderating variables (i.e. individual differences) such as experience using the Internet.

In a post-questionnaire, we asked a series of questions about response to the organization, site, and privacy policy specifically. All questions were measured on a ten-point Likert-style scale, with 0 – strongly disagree, 10 – strongly agree. We found that perception of the privacy policy clarity significantly correlates with perception of the policy, the site, and the organization.

We asked the participants to rate the clarity of the privacy policy in two questions ("The text of the privacy policy was easy to comprehend" and "The privacy policy clearly explains how my information will be used"). We combined these two measures into one value, Perceived Privacy Policy Clarity. We also asked participants to rate the level of trust they have in the privacy policy in two questions ("I believe the organization will keep my information confidential" and "The privacy policy increased the degree to which I trust the organization"). We combined these measures into one value, Privacy Policy Trust. It should be noted that the first questions are not about trust, merely perceived comprehensibility. The second set of questions deals directly with trust in the organization and its privacy policy.

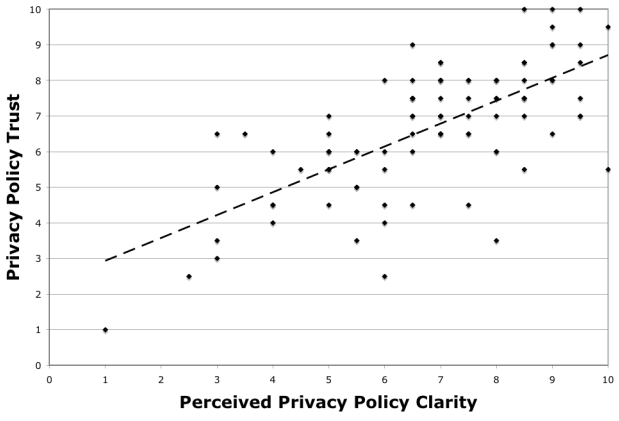

Figure 1. Perceived Privacy Policy Clarity Correlates to Privacy Policy Trust

As can be seen in Figure 1, there is a significant correlation (β=0.64, R^2=0.47, RMSD=1.45) between the Perceived Privacy Policy Clarity and Privacy Policy Trust.

We also compared Perceived Privacy Policy Clarity with another composite measure, Perceived Site and Organization

Credibility. The measure combines eight questions related to credibility of both the website and the organization that it represents. A strong correlation (β=0.67, R^2=0.73, RMSD=1.08) can be seen in Figure 2 between perceived clarity and overall site and organization credibility.

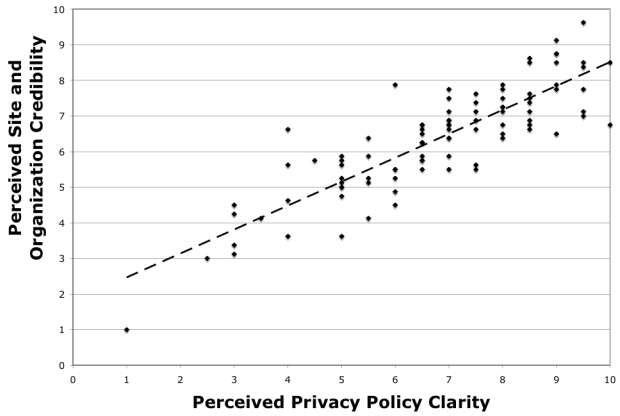

Figure 2. Perceived Privacy Policy Clarity Strongly Correlates with Overall Perceived Credibility

4. Privacy Policy Signature

Papacharissi & Fernback recommended that future research look for more items to indicate policy credibility. Along with Aristotle's *ethos* and Fogg's discussion of personal credentials as an important element leading to credibility, we hypothesized that having a signature on the privacy policy would lead to higher levels of trust and from there to greater willingness to share personal information.

As a result, we chose to manipulate the presence or absence of a signature at the end of the privacy policy (assigned randomly). We expected to see the results of this in a higher rate of participants in the signature condition giving personal information, either by signing a petition or joining a mailing list.

Unfortunately, both an ANOVA and a t-test revealed that the presence or absence of the signature did not alter the likelihood that a participant would share information. We chose to use a drawn signature (created with a tablet) to ensure visibility (see Figure 3). It is unlikely that the signature did not register visually or semantically, as recognition and comprehension times for words are typically below 500 ms [3]. As a result, we concluded that it is unlikely that a signature will motivate individuals to share personal information.

Figure 3. Signature of "Sam Appleby"

5. FINDINGS AND CONCLUSIONS

Privacy policies are necessarily legal documents; they must state in technical and definite legal terms what information will be collected, what will be protected, and how.

However, privacy policies are also agreements between (typically) an organization and an individual. Fewer than one in 400 Americans is a practicing lawyer, so ability to read this document is likely to be low. As our descriptive statistics for bank privacy policies show, these documents stretch the reading level of most Americans.

Given that these documents are legal in nature, one might suspect that they will necessarily be unreadable. Fortunately, there is some light at the end of the tunnel. One bank surveyed had privacy policy length of 1169 words, with a Flesch-Kincaid Grade Level of 8.9 and a Flesch Readability Ease of 52.7 – all more than one standard deviation from the mean.

We can reasonably conclude from our findings that privacy policy clarity will engender trust and confidence in the organization. Put simply, users do judge organizations on the basis of trust. If we can state that a usable privacy is understandable privacy, then organizations that wish to be trusted must make commitments to making privacy policies comprehensible.

While our initial theory led us to believe that trust might be engendered easily, through the addition of a signature to a privacy policy, that belief proved unwarranted. However, this is further encouragement for organizations to invest in long-term value strategy of making privacy policies comprehensible. The outlier bank mentioned above is a good example of this; one doubts that this large, successful bank produced a significantly more readable privacy policy by some accident.

6. FUTURE WORK

Performing scientifically valid tests of real privacy policies would be difficult. It is unlikely that any two privacy policies are completely legally equivalent, making comparisons problematic.

Instead, we intend to produce theoretically grounded design guidelines for comprehensible privacy policies, and subsequently to test these guidelines to provide empirical support. This is actually a complex undertaking: designing the guidelines will require input from literacy specialists, rhetoricians, privacy and security experts, and legal scholars, and testing the guidelines will require social scientists, as well. However, the value of this undertaking will be found (hopefully) in both better-educated consumers and more responsible organizations.

7. ACKNOWLEDGMENTS

Thanks to our participants, and to Shyam Sundar, Mary Beth Rosson, and Sampada Marathe.

8. REFERENCE

[1] Aristotle *On Rhetoric: A Civic Discourse*. Oxford University Press, 1992.

[2] Fogg, B.J. *Persuasive Technology*. Morgan Kaufmann, Boston, 2003.

[3] Holcomb, P.J. Semantic priming and stimulus degradation: implications for the role of the N400 in language processing. *Psychophysiology*, *30*. 47-61.

[4] Malhotra, N.K., Kim, S.S. and Argarwal, J. Internet users' information privacy concerns. *Information Systems Research*, *15* (4). 336-355.

[5] Papacharissi, Z. and Fernbeck, J. Online privacy and consumer protection: an analysis of portal privacy statements. *Journal of Broadcasting & Electronic Media*, *49* (3). 259-281.