Social Responsibility of Business For online privacy

Michael Fetick, 84270

Coleman University

**Social Responsibility of Business for Online Privacy**

Stakeholders want to know about: how a company upholds its social responsibilities, specifically, what it contributes to the public issues involving social, economic, environmental, innovation, and governance factors. One issue of importance is online privacy. Society believes that businesses should be responsible for the online privacy of their customers and partners in the course of doing business. The important factor of this responsibility is the availability and transparency of information concerning what the company is doing about protecting online privacy and security. As guidance, the Fair Information Practices (FIP) principles have been recognized by U.S. government agencies since 1974 in an effort to provide stakeholders protection. However, the recent proliferation of online data breaches calls to question the policies and practices of the businesses responsible for protection of the constituent data (Case, King, & Gage, 2015).

Online privacy continues to deteriorate, driven by a culture of self-revelation and also by powerful technologies for collecting personal information online without the knowledge or consent of users (Laudon & Traver, 2015).

**What is privacy on the Internet?**

Privacy is considered to be the moral right of individuals to be left alone, free from surveillance or interference from other individuals or organizations, including the state. Privacy on the Internet is referred to as online privacy or information privacy and is a subset of privacy. It includes both the claim that certain information should not be collected by governments or business firms, and the claim of individuals to control the use of whatever information is collected about them. Individual control over personal information is at the core of the privacy concept. Implicit in the claim to control one’s own personal information is the claim to be able to edit and even delete personal information from the Web (Laudon & Traver, 2015).

**Online Privacy and Security at the Fortune 500 Companies**

A study, which expanded upon previous studies, investigates the composition and usage of privacy policies of the Fortune 500 companies. Results showed that nearly all Fortune 500 firms post their privacy policy online with an increasing number of firms utilizing third-party compliance logos. Moreover, security techniques, data collection techniques, child data policies, and mobile application policies are now more commonly included and described in privacy policies. The usage of the FIP practices of notice/awareness, choice/consent, access/participation, and security/integrity, however, does vary and is changing (Case, King, & Gage, 2015).

A review of the Fortune 500 found that 450 firms (90%) have a posted privacy policy that is linked to the company’s homepage; 20 firms (4% of companies) have a policy on a page that is not hyper-linked to the homepage; resulting overall 94% of firms have an online policy. In terms of utilizing privacy logos, the most common logos are the U.S.-EU Safe Harbor logo (24 firms or 5% of companies) and the TRUSTe logo (23 firms or 5% of companies). In addition, the BBB Online logo is used by 11 (or 2%) of firms and the ESRB logo is used by 1 firm. Overall, 12% of companies utilize third-party privacy compliance firm logos. The study evaluated the content of posted policies according to the FIP guidelines: 91% provide notice/awareness within their policies; 81% include choice/consent, 76% describe access/participation, and 70% detail security/integrity. Two primary practices, for data collection and security techniques, were described within the privacy policies: 81% use cookies and beacons to collect data, 22% use SSL/TSL to enhance security during transmission. Additional policies provided the inclusion of mobile application policies by 30% of firms and the description of children data policies by 57% of firms (Case, King, & Gage, 2015).

**The Importance of Trust for Personalized Online Advertising**

Generic ads can lose effectiveness, so retailers employ a method called ‘retargeting’ to tailor their advertisements to the inferred interests and preferences of the individual consumer. This personalization should make the ad more appealing but its effectiveness depends on the consumer’s trust in the respective retailer. Personalization depth and breadth define a retargeting banner's ad personalization. For more trusted retailers, high-depth/narrow-breadth banners increase usefulness. In order to enhance the effectiveness of their online advertising retailers increasingly employ retargeting to tailor banners to individual consumers. Nevertheless, ad personalization has proven to be a delicate matter whose usage comes at the risk of triggering unfavorable responses (Bleier & Eisenbeiss, 2015).

**Thesis Peer Review**

This thesis paper was reviewed by a peer. The review was acknowledged with the following comments: Ms. Wenona Fetick says, “The paper has a good title and is well written.” She agrees that online privacy should be protected by the business who is handling your information.

# References

Bleier, A., & Eisenbeiss, M. (2015). The importance of trust for personalized online advertising. *Journal of Retailing, 91(3)*, 390-409. doi:http://dx.doi.org/10.1016/j.jretai.2015.04.001

Case, C. J., King, D. L., & Gage, L. M. (2015). Online Privacy and Security at the Fortune 500: An Empirical Examination of Practices. *ASBBS E-Journal (11.1)*, 59-67. Retrieved from http://search.proquest.com/docview/1699070593

Laudon, K. C., & Traver, C. G. (2015). *E-commerce 2015. Business. Technology. Society. 11th Edition.* Pearson Education, Inc.