Chapter 6.4
An Analysis of Online Privacy Policies of Fortune 100 Companies

Suhong Li
Bryant University, USA

Chen Zhang
Bryant University, USA

ABSTRACT

The purpose of this chapter is to investigate the current status of online privacy policies of Fortune 100 Companies. It was found that 94% of the surveyed companies have posted an online privacy policy and 82% of them collect personal information from consumers. The majority of the companies only partially follow the four principles (notice, choice, access, and security) of fair information practices. For example, most of the organizations give consumers some notice and choice in term of the collection and use of their personal information. However, organizations fall short in security requirements. Only 19% of organizations mention that they have taken steps to provide security for information both during transmission and after their sites have received the information. The results also reveal that a few organizations have obtained third-party privacy seals including TRUSTe, BBBOnline Privacy, and Safe Harbor.

INTRODUCTION

Privacy is defined as "the right to be let alone" which is part of the basic human rights to enjoy life (Warren, 1890). As an extension of privacy in the information age, information privacy is the legitimate collection, use, and disclosure of personal information, or "the claims of individuals that data about themselves should generally not be available to other individuals and organizations, and that, where data is possessed by another party, the individual must be able to exercise a substantial degree of control over that data and its use" (Clarke, 1999). One type of information privacy is online privacy, which is defined as "consumer concerns about what data is being collected by

DOI: 10.4018/978-1-61350-323-2.ch6.4

an online vendor about the customer and how it will be used" (Nyshadham, 2000). Compared to an off-line environment, the Internet enables organizations to collect more information from consumers cost effectively, sometimes even without the consent of consumers. The Internet poses greater security threats for consumers as their personal information is transmitted over the Internet if an organization does not have a good security mechanism in place. Furthermore, the connectivity of the Internet allows organizations to capture and build electronic profiles of consumers and potential consumers. Therefore, consumers today are facing a high level of privacy threat/invasion. One way to show an organization's commitment to protect consumers' online privacy is to post an online privacy policy and follow the policy truthfully. Online privacy has been viewed as a significant factor contributing to consumer trust and therefore an imperative for business success (Privacy & American Business, 2002). However, its provision is often at odds with organizational goals—such as the maximization of personal information value obtained from disclosure to third parties (often for commercial gain) and the retention of customer loyalty via enhanced personalized services (Lichtenstein, Swatman, & Babu, 2003).

The confrontation of individual versus organizational privacy prospective has started to drawn social and governmental attention. The Federal Trade Commission (FTC) has brought a number of principles to enforce the promises in organization's privacy statements (FTC, 1998; FTC, 2005). The FTC suggests a set of principles regarding collection, use, and dissemination of information which will ensure fair information practices. These principles include four core principles called notice, choice, access, and security. The implementations of these principles are as follows: first, organizations should tell consumers what information they collect and how it will be used (notice); second, consumers should be offered a choice about having their personal information used for other unrelated purposes or shared with third parties (choice); third, consumers should be able to review their personal information and have errors corrected (access); finally, organizations should protect the personal information they collect (security). If an organization follows all these principles, it can then be said to follow fair information practices (Nyshadham, 2000). Fair information practices have been used as a standard to evaluate the online privacy policy of organizations in several studies (Nyshadham, 2000).

Although online privacy issues have drawn social and governmental attention, the legislation of online privacy protection has not been fully implemented within the increasingly globalized e-commerce world. The European Union Directive on Privacy and Electronic Communications (EU Directive 2002/58/EC) has been adopted by EU. However, implementation of the EU directive by the member states has been slow because of resistance such as "considerable increase of the interest in the use (and retention) of traffic data by law enforcement authorities" (EDRI, 2004). Although the U.S. Federal Trade Commission (FTC, 1998) has published a guideline to enforce the promises in organization's privacy statements (FTC, 2005) and many bills related to consumer privacy are currently reviewed by the congress (CDT, 2005), the U.S. Online Privacy Protection Act is still in a proposal (Baumer, Earp, & Poindexter, 2004). As a result, the current online privacy protection legislations taken effect vary by industries and states. Among these, the Children's Online Privacy Protection Act (COPPA) and Health Insurance Portability and Accountability Act (HIPAA) have already taken effect (Desai, Richards, & Desai, 2003). The privacy provisions of the Gramm-Leach-Bliley Act (GLB Act) requires disclosure of a financial institution's privacy policy to consumers and requires that the institution provide the consumer an opportunity to opt out of any disclosures of non-public personal information to non-affiliated third parties (Wolf, 2004). The California Online Privacy Protect Act