IGI PUBLISHING

ITJ 4888

701 E. Chocolate Avenue, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.igi-global.com

This paper appears in the publication, International Journal of Information Security and Privacy, Volume 3, Issue 1
edited by **Hamid Nemati © 2009, IGI Global**

# Do Privacy Statements Really Work?

## The Effect of Privacy Statements and Fair Information Practices on Trust and Perceived Risk in E-Commerce

*Hamid R. Nemati, The University of North Carolina, USA*

*Thomas Van Dyke, The University of North Carolina, USA*

## ABSTRACT

*Companies today collect, store and process enormous amounts of information in order to identify, gain, and maintain customers. Electronic commerce and advances in database and communication technology allow business to collect and analyze more personal information with greater ease and efficiency than ever before. This has resulted in increased privacy concerns and a lack of trust among consumers. These concerns have prompted the FCC to call for the use of Fair Information Practices in electronic commerce. Many firms have added privacy statements, formal declarations of privacy and security policy, to their e-commerce web sites in an attempt to reduce privacy concerns by increasing consumer trust in the firm and reducing the perceived risk associated with e-commerce transactions. This article describes an experiment designed to determine the efficacy of that strategy.*[Article copies are available for purchase from InfoSci-on-Demand.com]

*Keywords: Electronic Commerce; Fair Information Practices; Privacy*

## INTRODUCTION

In today's highly competitive global marketplace e-commerce companies collect, store, and process enormous amounts of information. The marketing strategies of many successful firms increasingly depend on the use of detailed customer information to build relationships with current customers, attract new customers, and stimulate sales (Bessen, J., 1993; Culnan, M. J., & Armstrong, P. K., 1999). These strategies are abetted by the internet environment which allows business to collect and analyze more personal information with greater ease and efficiency than ever before. E-commerce firms use several methods to collect information about visitors to their sites. These methods include registration forms, web surveys, order forms and cookies. The information thus gathered serves as an important input into marketing, advertising, customer service and product-related decisions made by on-line retailers. However, the collection of this information creates the risk of possible misuse and generates concerns over information privacy. In a report to congress the FTC cited a survey showing that 92% of households with Internet access stated that they do not trust online companies to keep their personal information confidential (Federal Trade Commission, 2000).

These privacy concerns reflect a lack of trust that has serious negative impact on e-commerce (Hoffman, D. L., Novak, T. P., & Peralta, M., 1999). In a survey by AC Neilson, consumers rated the disclosure of personal information and security issues concerning using a credit card online as the biggest barriers to online purchasing (ACNielson). Because of these concerns, many consumers simply refuse to make purchases online. The Federal Trade Commission estimates that on-line retail sales in 2003 were reduced by up to $18 Billion due to concerns over privacy (2000).

While considerable progress has been made in the development of technological mechanisms for secure payment, they have done little to alleviate privacy concerns.

There is evidence that consumer's concerns about privacy risks associated with e-commerce are justified. In January 2000, the merger of the online advertising company DoubleClick and the database marketing firm Abacus Direct started a federal investigation when it was revealed that the company had compiled profiles of over 100,000 online users, without their consent, and intended to sell the information (Kristol, D. M., 2001). More recently, the FTC reported 214,905 instances of identity theft in 2003. This represented 42% of all complaints up from 40% in 2002 (Federal Trade Commission). Clearly, some threats to privacy and security related to internet shopping and on-line information gathering are real.

It is clear that consumers do not trust companies to keep their personal information private and they do not trust internet technology to secure their financial transactions (Hoffman, D. L., Novak, T. P., & Peralta, M., 1999). This lack of trust is costing e-retailers billions in lost sales. As an article in the Wall Street Journal put it "It seems that trust equals revenue, even on-line (Petersen, A., 2001). It is trust that must be created in order to counter the effects of privacy and security concerns. Two factors must be balanced in order for a customer to do business with an online vendor. Customer trust in the firm must be high enough and the perceived risk associated with performing the transaction over the internet must be low enough to meet the comfort threshold of the consumer before that consumer will disclose information and engage in an e-commerce transaction with a specific vendor.

The purpose of this investigation is to determine the efficacy of using privacy statements to alleviate customer's privacy concerns related to e-commerce. In this article we examine the pattern of change in perceived risk and customer trust related to the reading of privacy statements. We also investigate the effect of varying the content of privacy statements. Specifically,