IDEA GROUP PUBLISHING
701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com
ITB12628

This paper appears in the book, *Emerging Trends and Challenges in Information Technology Management, Volume 1 and Volume 2* edited by Mehdi Khosrow-Pour © 2006, Idea Group Inc.

A Descriptive Study of Online Privacy in the GCC Countries

Zeinab Karake Shalhoub, Professor of MIS, American University of Sharjah, PO Box 26666, Sharjah, UAE,
T: 971-6-515-2309, zkarake@aus.edu

INTRODUCTION

It is always difficult to analyze privacy and security as a phenomenon and may be almost impossible to analyze trust in the context of electronic commerce because of the complexity of electronic commerce. However, trust will be the decisive factor for success or failure of e-businesses. It is therefore vitally important for companies doing business online to act in a way that engenders consumers' trust. Karake Shalhoub (2002) has studied a number of US based pure play firms to determine what she labeled *trust enhancers*. Her findings identified two main categories: Privacy and Security as the main determinants of trust in electronic commerce.

The United States Federal Trade Commission (FTC) has been studying the issue of online privacy in the commercial sector since 1995. In its initial report on online privacy, issued in 1998, the FTC recommended that Internet privacy issues be addressed through industry self-regulation and identified the core principles of privacy protection common to domestic and international documents describing fair information practices: notice, choice, access and security (FTC, 1999). The FTC recommended that commercial websites exhibit some sensitivity to privacy concerns and a determination to self-regulation by including a privacy statement, which addresses all of the core privacy principles. More recently, the FTC has also recommended participation in online privacy seal programs. These programs require licensees to implement certain fair information practices and submit to compliance testing in order to display a privacy seal on their websites.

Specifically, the FTC proposed and advocated that fair information practices (FIPs) included the following dimensions: Notice/Awareness, Access, Choice, Security, and Enforcement and Redress. These widely recognized set of topics to address when a party in a transaction manipulates data about an individual.

An equally important contributor for e-business in general and trust in particular is the perceived security aspect. In the early days of e-business consumers avoided doing business online mainly because of security concerns. Recently many developments have taken place to ease customer fear of the security problem online; the development of the concept of secure sockets layer (SSL) was introduced. Directly, pure play and brick and mortar firms, like Amazon.com, took advantage of the security provided by SSL and grew quickly (Srinivasan, 2004).

Another instrument available today for enhancing trust is the digital certificate. Digital certificates are electronically verified. The Cheskin Research Group (1999, 2000) found that the existence of logos of the firms (such as VeriSign) will contribute to the level of trust in online business. VeriSign falls in the Trusted Third Party (TTPs) category; TTPs are organizations whose main objective is to raise consumers' trust in online transactions.

Table 1. Distribution of sampled firms among the six countries

Country	Number of Companies	Percentage
Bahrain	10	5.46 %
Kuwait	16	8.74 %
Oman	11	6.01 %
Qatar	9	4.92 %
Saudi Arabia	74	40.44 %
UAE	63	34.43 %

This paper covers a descriptive study of the privacy issues of a sample of companies from the six countries of the GCC which are engaged in electronic commerce transactions.

In what follows, the author will describe the sample of companies chosen from the six countries; then, a descriptive analysis of the privacy statements of the sample companies will follow. The paper will conclude with a summary section and suggestions for future research.

THE SAMPLE

This study, and for the first time, covers a sample of Web sites in a group of developing economies, namely the six countries of the Gulf Cooperation Council. The author evaluated 183 popular commercial Web sites based on the FTC specifications. In evaluating the Web sites the following questions were examined:

1. How many GCC companies have privacy policies on their Web sites?
2. Are privacy policies different among industry types?
3. What is the content of online privacy policy statements?
4. To what extent do the Web sites address each of the five FTC privacy dimensions?

The methodology involved a content analysis of information from 183 companies' public Web sites. These Web sites were identified and classified based on the Standard Industrial Classification (SIC)/North American Industry Classification System (NAICS), as classified by the AMEinfo Business directory. Table 1 contains the distribution of the sample by country.

Table 2. Web sites classified by industry

Industry Type and SIC Classification	Number of Sites	Sites with Privacy Policy	Percentage with Privacy Policy
Accommodation and Food Services	6	1	16.7 %
Administrative and Support and Waste Management and Remediation Services	0	0	0
Agriculture, Forestry, Fishing and Hunting	2	0	0
Arts, Entertainment, and Recreation	2	0	0
Construction	5	0	0
Educational Services	3	1	33.3%
Finance and Insurance	36	13	36.1 %
Health Care and Social Assistance	14	3	21.4 %
Information	11	6	54.5 %
Management of Companies and Enterprises	0	0	0
Manufacturing	21	5	23.8 %
Mining	6	0	0
Other Services (except Public Administration)	0	0	0
Professional, Scientific, and Technical Services	0	0	0
Public Administration	16	6	37.5 %
Real Estate and Rental and Leasing	0	0	0
Retail Trade	41	10	24.4 %
Transportation and Warehousing	2	0	0

As can be seen from table 1, Saudi Arabia and the UAE comprise close to 75 percent of the Web sites examined. This is consistent with the fact that the two countries have the largest numbers of registered Internet hosts (ITU, 2004).

The distribution of Web sites per industry, along with the number of sites with privacy policy is depicted in table 2. The classification was based on the 1997 North American Industry Classification System (NAICS), which was updates of the original Standard Industrial Classification (SIC) (OMB, 1997).

ANALYSIS OF PRIVACY POLICIES

The list of the 183 Web sites is diversified and contains the leading companies in the Gulf region. The privacy policies for each of the 183 Web sites were examines. Most policies were conveniently located with a privacy hyperlink on the home page of the site (85.4 %). Overall the survey showed that only 26.8 percent, or 49 sites out of the total sample of 183 had a privacy statement and only 22.9 percent of the Web sites had some type of privacy policy posted as a link from their home page. Table 3 provides a summary of the findings.

A content analysis of the examined Web site privacy policies identified which dimensions of privacy were addressed. A large percentage of Web sites with privacy policy (71.6% or 19.2 percent of the total sample) had some information on the notice or awareness dimension. This dimension is stressed by the FTC as the most important dimension of the privacy policy. Those surfing the Web should be notified that the site is collecting information related to their surfing activities.

Information on choice and consent were contained in 70.9 percent of sites with privacy policy or 19 percent of the total sample. This deals with giving consumers options as to how any personal information collected from them may be used.

Information regarding access and participation were displayed on 33 percent of the privacy statements (9 percent of the total sample, or 16 sites only), while information on security and integrity of the data collected and kept was addressed by 28.7 percent of the privacy statements (7.6 percent of the total sample or only 14 sites only).

As with respect to the Enforcement and Redress dimension, none of the sites has a provision to inform users in case of any complaint, as to whom they should address their complaint, what is the arbitration and settlement methods, who is the enforcement body and finally what are the penalties and sanctions applicable. It is troubling to find that enforcement in this environment is virtually non-existent. But our finding is consistent with findings in the United States whereby most industry-promulgated guidelines have minimal enforcement mechanisms, and the standard penalty for breaching the practices recommended by a third-party privacy organization is removal of its privacy seal icon from the offending Web site. Affected customers and users have no means of legal redress against companies that violate self-regulatory principles (Henderson, 2005).

Table 3. Summary of findings

	Description	%
-	No Privacy Statement available	73.2 %
-	Privacy Statement; website contains Privacy Statement	26.8 %
-	Privacy Statement link from home page	22.9 %
1.	Notice and Awareness	19.2. %
2.	Choice and Consent	19.0 %
3.	Access and Participation	9.0 %
4.	Security and Integrity	6.3 %
5.	Enforcement and Redress	0.0 %
1. 2.	Notice and Awareness Choice and Consent	17.0 %
1. 2. 3.	Notice and Awareness Choice and Consent Access and Participation	12.5 %
1. 2. 3. 4.	Notice and Awareness Choice and Consent Access and Participation Security and Integrity	7.1 %
1. 2. 3. 4. 5.	Notice and Awareness Choice and Consent Access and Participation Security and Integrity Enforcement and Redress	0.0 %

CONCLUSION

There are no regulations in the GCC dealing with privacy or privacy issues, in general. The UAE enacted an Electronic Transactions and Commerce Law in 2002 which deals with digital signatures and electronic registers. It prohibits ISPs from disclosing information gathered in providing services. The penal code also contains some provisions; it does not address cybercrime or data protection, though. It is worthwhile mentioning that a cyber-crime act is currently being developed in the UAE.

As the GCC societies move away from cash-based to credit based, it is expected that e-commerce and e-business transactions will increase. To assure customers that their privacy is being protected and to increase their level of trust, it is imperative for public sites to develop and publish online privacy policies. As privacy concerns increase in importance, businesses should show that they understand the issue and they do care about customers' privacy.

Based on our knowledge of the Gulf region, firms in the GCC countries need to see the e-economy as a way to increase revenue and improve efficiency. This is extremely important given the fact that a large percentage of firms are family owned businesses that contribute greatly to job growth, especially in the past five years. Measures to stimulate greater use of electronic technology, especially electronic commerce include government initiatives in enacting legislation to protect personal information and consumer electronic activities. The GCC governments need also to form comprehensive e-strategy for building the base for e-economies and addressing the adoption and diffusion of electronic commerce in key economic sectors.

Another recommendation is for the private sector to take an active role in reaching an acceptable level of e-readiness in the GCC countries. Private sector firms must do more to drive electronic business and electronic commerce use among partners, suppliers and distributors. In addition, private sector firms and public policy makers must all work together and formulate private-public sector initiatives to address security concerns.

REFERENCES

Cheskin Research Group (2000). Trust in the wired Americas. Available from the World Wide Web at http://www.cheskin.com/think/studies/trust2.html.

Cheskin Research Group (1999). eCommerce trust study. Available from the World Wide Web at http://www.cheskin.com/think/studies/ecomtrust.html.

Federal Trade Commission (1999). "Self-regulation and privacy online: A report to Congress," Available at www.ftc.gov/reports/privacy99/privacy99.pdf

Henderson, B.R. (2005)."Opt in or opt out: Are these the only options?" *Journal of Internet Law.* 18(11): 1-8.

International Telecommunication Union (2004). ITU Digital Access Index: World's First Global ICT Ranking. Published by ITU, Geneva: Switzerland.

Karake Shalhoub, Z. and Al Qasimi, L (forthcoming). Electronic Commerce Diffusion in Developing Economies: A Resource Based Perspective. Edgar Elgar Publishing.

Karake Shalhoub, Z. (2002). Trust and Loyalty in Electronic Commerce: An Agency Theory Perspective. Quorum Publishing, New York: New York.

Office of Management and Budget. 1997. North American Industry Classification System, United States.

Srinivasan, S. (2004). "Role of trust in e-business success," *Information management and Computer Security,* 12(1): 66-73.