Antecedents And Consequences Of Consumers' Online Privacy Concerns

Soumava Bandyopadhyay, Lamar University, USA

ABSTRACT

This paper proposes a theoretical framework to investigate the factors that influence the privacy concerns of consumers who use the Internet, and the possible outcomes of such privacy concerns. Factors identified as antecedents to online privacy concerns are perceived vulnerability to personal data collection and misuse, perceived ability to control data collection and subsequent use, the level of Internet literacy, social awareness, and background cultural factors. The possible consequences of online privacy concerns are the lack of willingness to provide personal information online, rejection of e-commerce, or even unwillingness to use the Internet. Managerial implications of the framework are discussed.

Keywords: Internet, online privacy, e-commerce

INTRODUCTION

Invasion of privacy on the Internet involves the unauthorized collection, disclosure, or other use of personal information (Wang, Lee, and Wang, 1998). As e-commerce continues to grow worldwide, companies are gathering an increasing amount of personal information from consumers on the Internet. Private information on consumers is now a commodity that is routinely bought, sold, and traded (Gillmor, 1998). Such information could be obtained voluntarily (when consumers provide information during online transactions or while registering to use certain Websites) or involuntarily (by use of cookies that track consumers' online surfing behavior) on the part of consumers. Marketers across the board now collect detailed individual-level information to profile consumers, and increase the efficiency and effectiveness of their marketing strategies. It is now virtually impossible for consumers to transact business online without having to reveal personal information (Rust, Kannan, and Peng, 2002). Vast amounts of individual information can be very easily collected over the Internet, and digital networks can link all this private information in databases (Caruso, 1998). Consequently, consumer concerns regarding having to reveal personal information online and regarding the way in which organizations collect and use such information is also on the rise (Fletcher, 2003). Such concerns range from just intrusion of one's privacy to potential hassles stemming from online identity theft. Online privacy concerns are felt globally, as the Internet is a global medium, and allows the transfer of massive amounts of consumer information instantly across national borders (Nijhawan, 2003). Researchers have identified factors such as awareness of information collection, perceived vulnerability to information misuse, experience with Internet use, cultural background of consumers, etc. to be antecedents to consumers' online privacy concerns (Sheehan and Hoy, 2000; Dinev and Hart, 2004; Bellman et al., 2004). The consequences of such concerns about privacy could range from consumers declining to provide personal information online to the outright rejection of e-commerce, or even minimizing the use of the Internet (Nam et al., 2006; Dinev and Hart, 2006a).

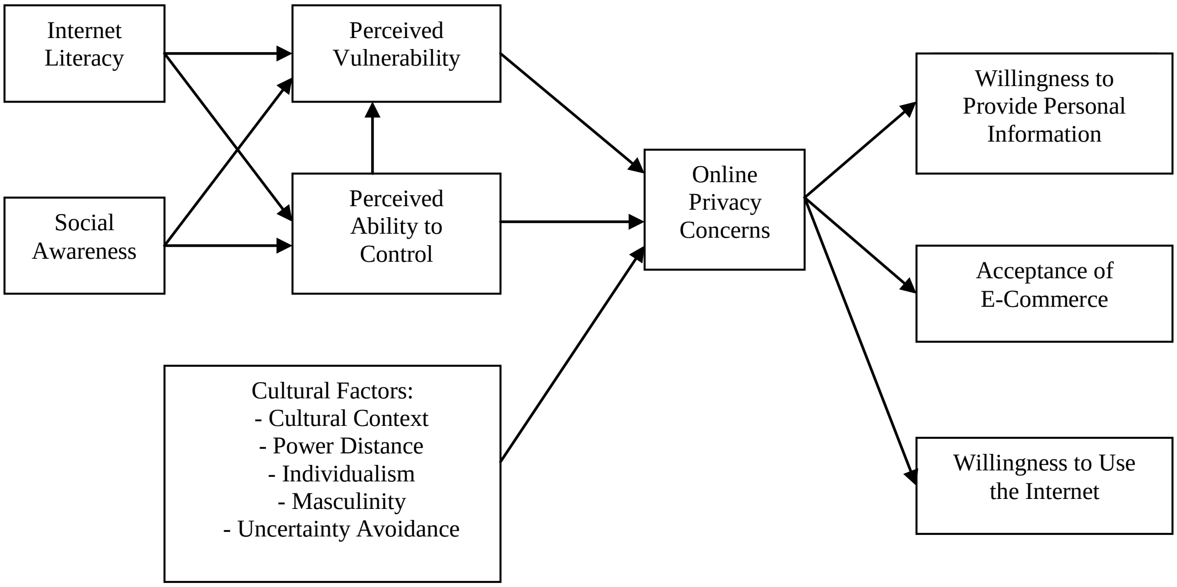
Research on consumers' online privacy concerns has so far been characterized by isolated efforts to identify and discuss only a few factors that impact and stem out of such concerns. This paper proposes a conceptual framework that includes a comprehensive set of antecedent and consequent factors. In developing the framework, we have integrated the works of previous researchers, as well as proposed a few additional factors, and new relationships between these factors and consumer concerns regarding online privacy. Following the description of the framework, the paper offers some managerial implications in terms of reducing consumers' online privacy concerns and encouraging e-commerce.

THE FRAMEWORK

The proposed framework is presented in Figure 1. Three main antecedent factors are seen to influence consumers' online privacy concerns. These are: perceived vulnerability to information misuse, perceived ability to control the release and use of private information, and characteristics of the consumer's cultural background. The perceived vulnerability to information misuse, and the perceived ability to control information use are both influenced, in turn, by two factors, the consumer's level of Internet literacy, and the consumer's social awareness about the Internet. Depending on the degree to which a consumer is worried about online privacy, three levels of consequences are possible: unwillingness to reveal personal information online, unwillingness to enter into e-commerce transactions, or even unwillingness to use the Internet altogether.

Figure 1

The Proposed Framework



ANTECEDENTS OF ONLINE PRIVACY CONCERNS

Perceived Vulnerability

Consumers' perceived vulnerability to the misuse of personal information obtained online as a major antecedent of online privacy concerns was proposed by Dinev and Hart (2004). *Perceived vulnerability* describes the perceived potential risk when personal information is revealed (Raab and Bennett, 1998). The revelation of private information could be caused by many factors, such as accidental disclosure, unauthorized access, hacking into networks, etc. (Rindfleish, 1997). The possible negative consequences for consumers include identity theft (Saunders and Zucker, 1999), undesirable consumer profiling (Budnitz, 1998), and being targeted by unwanted advertising messages on the Internet (i.e., 'spam' e-mails). These factors contribute to consumers feeling increasingly vulnerable to the risk of misuse of their private information on the Internet and, therefore, experiencing increased online privacy concerns (Dinev and Hart, 2004).

Perceived Ability to Control

Consumers may try to neutralize the risk of possible negative consequences of information misuse by controlling the manner in which their personal information is collected and used. *Perceived ability to control* is the extent to which consumers think that they can withhold personal information from being disclosed online, which allows them to exercise their right to privacy (Dinev and Hart, 2004). According to Culnan and Armstrong (1999), consumers perceive information disclosure as less invasive of their privacy when they believe that they can control when and how such information is disclosed and used in the future. This is the concept of 'procedural fairness' in the practice of collecting consumer information. The Federal Trade Commission has identified five core principles to guide privacy policy development by online content providers (Sheehan and Hoy, 2000). These principles are:

1. *Notice*: Consumers should be made aware of a Website's information collection and usage practices before information is collected.
2. *Choice*: Consumers should be allowed to choose participation or exclusion of the collection of personal information.
3. *Access*: Consumers should have access to their personal information and should be able to correct erroneous information.
4. *Security*: Policies to ensure the integrity of data and the prevention of misuse should be in place.
5. *Redress*: Enforcement mechanisms should be in place to ensure compliance with the above principles. Such mechanisms could include self-regulation or government regulation.

The FTC guidelines described above enable online consumers to control the collection and use of their personal data. If consumers feel convinced by the stated privacy policy of a Website that they can control the collection and usage of their private information by that site, they will tend to trust that site. Another element that may increase consumer trust and confidence on a Website is the use of third-party online seal of approval programs, such as TRUSTe and Verisign, that reflect the site's respect for personal privacy (Miyazaki and Krishnamurthy, 2002). Building trust help in reducing consumer privacy concerns with a Website (Milne and Boza, 1999; Nam et al., 2006), and a major determinant of such trust is the consumer's perceived ability to control the gathering and use of personal information. Therefore, consumers' online privacy concerns are likely to be reduced by their perceived ability to control information collection and dissemination.

There is also a relationship between the perceived ability to control personal information collection and usage, and the perceived vulnerability to information misuse. If consumers feel that they can actually control how their private information is collected and used by Websites, they will also feel less vulnerable to the potential negative outcomes of information misuse. Therefore, perceived ability to control private information flow on the part of consumers will reduce their perceived vulnerability and, in turn, will reduce their online privacy concerns.

Internet Literacy and Social Awareness

The role of Internet literacy and social awareness in influencing online privacy concerns was proposed by Dinev and Hart (2006a). *Internet literacy* refers to the level of skill and knowledge possessed by consumers in using the Internet, including establishing an Internet connection, navigating the Web, completing e-commerce transactions, protecting the computer from viruses and spyware, setting the browser's privacy and security options appropriately, and protecting one's privacy by employing adequate measures before disclosing information online (Dinev and Hart, 2006a; Spiekermann, Grossklags, and Berendt, 2001). In the context of our research, s*ocial awareness* is described as the extent to which consumers are knowledgeable about the social issues involving Internet usage (Dinev and Hart, 2006a), such as trust, privacy, security, governance, censorship, and restrictions (Burn and Loch, 2001; Papazafeiropoulou and Pouloudi, 2001). Social awareness requires raised interest and passive involvement in these social issues, and is a key in increasing consumer consciousness (Bickford and Reynolds, 2002). Consumers who are socially aware will be interested in and follow community and government policies and initiatives related to technology and the Internet. Because of their interest in social issues and policy, consumers with a high degree of social awareness will closely follow Internet privacy issues and the development of privacy policies and regulations (Dinev and Hart, 2006a).

Previous research has suggested that Internet literacy and social awareness directly and positively impact online privacy concerns (Dinev and Hart, 2006a). In our model, we propose that the effects of Internet literacy and social awareness on privacy concerns are indirect, via the previously described factors of perceived vulnerability and perceived ability to control (as shown in Figure 1). We also propose that the eventual impact of Internet literacy and social awareness on privacy concerns will be positive or negative, depending on the specific skills and knowledge gained through such literacy and awareness. If a consumer's Internet literacy and social awareness makes him knowledgeable about the many ways (e.g., tracking cookies, spyware, hacking, etc.) in which his privacy could be intruded upon, he will feel more vulnerable to losing his privacy on the Internet and, consequently, his online privacy concerns will increase. On the other hand, the level of Internet literacy that a consumer has may enable him to adequately protect himself by using Internet security software, setting up firewalls, not granting permission to Websites to transfer personal data, and other similar means (Bellman et al., 2004). The social awareness of the consumer may make him knowledgeable about the legal protection available from the consequences of personal data misuse (e.g., limited financial liability from fraudulent online credit card transactions owing to online identity theft), and about the federal guidelines (or any other regulatory protection available in the consumer's country) regarding Website privacy policy development and specific rights of consumers. Such a level of Internet literacy and social awareness will make consumers feel that they would be able to adequately control the collection and use of their personal information, and that will in turn reduce their perceived vulnerability to the loss of privacy. Subsequently, their online privacy concerns will be reduced.

Cultural Factors

The influence of national cultural characteristics on online privacy concerns has been recognized (Bellman et al., 2004), but has so far remained largely unaddressed by researchers. Our premise is that for a global medium such as the Internet, a consumer's cultural surroundings or background would have a significant influence on his attitudes and behaviors leading to concern for online privacy. In our framework, two established indicators of national cultural values are identified as determinants of the extent to which consumers in a particular country will be concerned about their online information privacy. These are Hall's (1976) cultural context, and Hofstede's (1980) cultural dimensions (Power Distance, Individualism, Masculinity, and Uncertainty Avoidance). Cultural context (Hall, 1976) explains the elements that help people understand communication-related behavioral norms in a society. In high-context cultures, the contextual elements of communication, rather than the actual words, are more important. As a result, much is taken for granted, based on the trust factor. In low-context cultures, on the other hand, communication is explicit, and contextual elements are not as important. Hofstede's (1980) cultural dimensions have been widely used for research studies of social values suggesting that the cultures of different nations can be compared in terms of these dimensions (Keegan and Green, 2008).

Cultural Context

In low-context cultures (e.g., United States, Germany), people prefer to maintain a bubble of private space and resent intrusions, whereas high-context cultures (e.g., Japan, the Arab world, Latin America) have a relatively less emphasis on private space (Hall, 1976). This is because building of interpersonal trust is a critical prerequisite for meaningful communication in high-context cultures, and these cultures tend to maintain that such trust cannot be generated if people remain within themselves and emphasize privacy. Therefore, consumers in low-context cultures are likely to be more concerned with online privacy than consumers in high-context cultures.

Power Distance

In high power distances cultures (e.g., China, France), less powerful members of the society accept power to be distributed unequally (Hofstede, 1980). This is often manifested in people's unquestioned acceptance of authority. Therefore, in high power distance cultures, people are more likely to tolerate giving up their privacy to authorities than in low power distance cultures (e.g., Germany, Scandinavia), where power is more equally distributed within the society. As a result, we expect that consumer concerns for online privacy will be negatively related to the power distance index of a culture.

Individualism

Each member in an individualist culture (e.g., United States, Western Europe) is more concerned about his or her own interest, whereas people in a collectivist culture (e.g., Japan and other Asian countries) are integrated into cohesive in-groups (Hofstede, 1980). Individualism is associated with personal time, freedom on the job, challenge, and individual responsibility, whereas collectivism puts more stress on a supportive work environment and group responsibility. Low individualism, or collectivist, societies, then, are likely to be more tolerant of groups intruding on the privacy of the individual (Bellman et al., 2004). An individualistic cultural orientation is more likely to appreciate the motto of "do your own thing," and this should lead to greater awareness and concern for privacy. Therefore, we propose that consumer concerns for online privacy will be positively related to the individualism index of a culture.

Masculinity

Hofstede (1980) noted that highly 'masculine' cultures (e.g., Japan, Austria, Italy) tended to promote the values of assertiveness, and material success than in more 'feminine' cultures (e.g., the Netherlands, Spain, Denmark, Sweden). Masculinity reflected the degree to which societies subscribed to the typical stereotypes associated with males and females. Therefore, masculine societies stress values such as productivity and competition, while feminine societies emphasize quality of life, social welfare, and cooperation. The greater emphasis on achievement and material success in masculine cultures may create a greater appreciation for the economic benefits of private information use (Bellman et al., 2004). Therefore, consumer concerns for online privacy are likely to be positively related to the masculinity index of a culture.

Uncertainty Avoidance

Cultures characterized by high uncertainty avoidance (e.g., Greece, Portugal, Belgium) are uncomfortable with unclear, ambiguous and unstructured situations (Hofstede, 1980) than those characterized by low uncertainty avoidance (e.g., Ireland, Sweden, the United Kingdom, India). Societies manifesting high uncertainty avoidance emphasize explicit rules and regulations, long range planning, and reliance on information systems. Societies with low uncertainty avoidance exhibit fewer rules, less reliance on information systems, and less need for long range planning. Acceptance of uncertainty generally leads to behavior that is more contemplative, relativistic, and tolerant, while strong uncertainty avoidance may be expressed through aggressive and intolerant behavior (Keegan and Green, 2008). To reduce uncertainty, people in cultures having a high uncertainty avoidance index are likely to be more protective of private information. They would not like to divulge information if they are not sure of who would collect their private information online and/or how that information might be used in the future. Hence, we propose in our framework that consumer concerns for online privacy will be positively related to the uncertainty avoidance index of a culture.

CONSEQUENCES OF ONLINE PRIVACY CONCERNS

Heightened consumer concerns about online information privacy is likely to affect all Internet-based activities that could result in the collection and subsequent of personal data. When consumers perceive that negative consequences could result from submitting personal data online, they are less likely to do so (Nam et al., 2006). Depending on the degree of concern consumers have about online privacy, three levels of outcome are possible: 1) refusing to provide personal information on the Internet, 2) refusing to enter into e-commerce transactions where personal information is asked for; and 3) refusing to use the Internet altogether in fear of privacy violation.

Willingness to Provide Personal Information

At the minimal level, consumers who are concerned about their online privacy will be unwilling to disclose personal information to Websites (Nam et al., 2006). This may result in browsing Websites where no personal data is captured (Rice, McCreadie, and Chang, 2001), or providing only limited and anonymous, or even false personal information to Websites (Dinev and Hart, 2006b) that require "registration" to use content.

Acceptance of E-Commerce

Consumers with elevated online privacy concerns could be unwilling to make e-commerce transactions altogether, since almost all such transactions require the disclosure of sensitive personal information, such as credit card numbers, telephone numbers, e-mail and postal addresses, etc. (Dinev and Hart, 2006a). Graeff and Harmon (2002) reported a survey where nearly three-quarters of the respondents said that they did not feel comfortable using their credit cards for online purchases.

Willingness to Use the Internet

Unwillingness to use the Internet altogether because of online privacy concerns is likely to be seen in extreme cases. Consumers who are very highly concerned about protecting their privacy online may realize that even if they do not voluntarily submit any personal information to a Website, information is still exchanged between the consumers' client computers and the host server of the Website. The information exchanged includes the client machine's IP address (leading to the identification of the site user's location), and details of the specific areas of the Website that have been visited. A recent case involving AOL, the Internet service provider, has revealed that Internet users can be identified only by their online search activity records (Barbaro and Zeller, 2006). Some Websites install software (known as "spyware") on client machines without the users' knowledge and consent. This software monitors the users' Web surfing activities and provides the information to a specific server (Staples, 2004). While the planting of spyware without the user's awareness and consent is illegal, many legitimate Websites install small files called "cookies" on user's hard drives for relatively benign purposes, such as letting the user personalize the Website, identifying registered users of a Website, recall stored shopping cart information at e-commerce sites, etc. Although legitimate Websites install cookies only with the user's permission (typically stated in their privacy policy), and they can be configured to run on Web browsers only under the user's own settings, the cookies are normally executed without any user action (Strauss, El-Ansary, and Frost, 2006). This feature is startling to Internet users who are extremely concerned about online privacy, and may feel that they could be unknowingly and involuntarily disclosing sensitive information while online. To protect their privacy, these consumers may heavily limit their Internet surfing behavior.

MANAGERIAL IMPLICATIONS

The negative consequences of consumers' online privacy concerns are not acceptable to marketers who rely on enhancing their marketing strategies (consumer profiling, better targeting, etc.) by collecting and analyzing individual-level data, or who offer e-commerce transactions on their Websites. To reduce the probabilities of all three negative outcomes identified in our framework, marketers will need to address the antecedents of online privacy concerns and alleviate those concerns.

The framework suggests that online privacy concerns could be reduced by increasing the consumers' perceived ability to control the collection and use of sensitive personal information, and by reducing their perceived vulnerability to information misuse and its consequences. Legitimate marketers may do this by adhering to the FTC guidelines for privacy policy development that have been described earlier in the paper, and posting a comprehensive privacy policy prominently on the home page of the Website (Hui, Teo, and Lee, 2007). This will increase the social awareness of Internet users, which will help in increasing the perceived ability to control information and the perceived vulnerability to information misuse. A key element is to convince the consumers regarding the procedural fairness in the collection and use of personal data, and increasing the consumers' trust in the Website (Culnan and Armstrong, 1999). Specific measures that marketers may implement include promoting the reputation and legitimacy of the company requesting information (Andrade, Kaltcheva, and Weitz, 2002), displaying third-party privacy seals such as BBBOnline, TRUSTe, etc. on their Websites (Hui, Teo, and Lee, 2007). It is also prudent for online marketers not to ask for more information than is absolutely necessary for effecting e-commerce transactions.

Marketers should also make efforts to increase consumers' Internet literacy by educating them about the options available for protecting private information. For example, they can post information on their Websites about specific software (e.g., firewalls, browser security fixes) or procedures (e.g., setting browser configurations to prevent tracking cookies being implanted without the user's permission) that may alleviate privacy concerns by increasing the perceived control and reducing the perceived vulnerability (Spiekermann, Grossklags, and Berendt, 2001).

The cultural factors that have been identified as antecedents to online privacy concerns are of relevance to online marketers who operate across borders. The extent to which marketers need to address the privacy concerns of consumers in a particular culture depends on the attitudes of Internet users in that culture toward online privacy, and the degree to which that cultural setting influences online privacy concerns. For example, in cultures where online privacy concerns are relatively low (e.g., Japan, France, India), marketers will need to employ relatively less effort in reducing consumers' privacy concerns to boost e-commerce transactions compared to cultures where online privacy concerns are relatively high (e.g., the United States, Germany).

CONCLUSION

This paper presents a comprehensive theoretical framework that identifies the antecedent factors to consumers' online privacy concerns and the interrelationships among those factors. Online marketers need to understand these factors and address them appropriately, so that consumers' online privacy concerns are reduced and they are willing to disclose personal information on the Internet, and engage in e-commerce transactions. The next logical step is to empirically test the relationships proposed in the study, and validate the framework. The empirical testing should be carried out with diverse consumer groups, and across cultures, so that global differences in the importance and applicability of the factors are also identified.

AUTHOR INFORMATION

Soumava Bandyopadhyay is a professor of marketing at Lamar University, U.S.A. He received his Ph.D. from The University of Alabama. His areas of research interest include interactive marketing, global marketing, and channels of distribution.

REFERENCES

1. Andrade, E.B., Kaltcheva, V., & Weitz, B. (2002). Self-Disclosure on the Web: The Impact of Privacy Policy, Reward, and Company Reputation. *Advances in Consumer Research*, 29, 350-353.
2. Barbaro, M. & Zeller, T. (2006). A Face is exposed for AOL Searcher No. 4417749. *New York Times*, August 9.
3. Bellman, S., Johnson, E.J., Kobrin, S.J., & Lohse, G.L. (2004). International Differences in Information Privacy Concerns: A Global Survey of Consumers. *The Information Society*, 20, 313-324.
4. Bickford, D.M. & Reynolds, M. (2002). Activism and Service-Learning: Reframing Volunteerism as an Act of Dissent. *Critical Approaches to Teaching, Literature, Language, Composition, and Culture*, 8 (2), 229-252.
5. Budnitz, M. (1998). Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation is Inadequate. *South Carolina Law Review*, 49 (1), 847-886.
6. Burn, J. & Loch, K. (2001). The Societal Impact of the World Wide Web—Key Challenges for the 21st Century. *Information Resources Management Journal*, 14 (4), 4-14.
7. Caruso, D. (1998). The Law and the Internet Beware. *Columbia Journalism Review*, 37 (1), 57-61.
8. Culnan, M. & Armstrong, P. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science*, 10 (1), 104-115.
9. Dinev, T. & Hart, P. (2004). Internet Privacy Concerns and Their Antecedents—Measurement Validity and a Regression Model. *Behavior and Information Technology*, 23 (6), 413-422.
10. Dinev, T. & Hart, P. (2006a). Internet Privacy Concerns and Social Awareness as Determinants of Intention to Transact. *International Journal of Electronic Commerce*, 10 (2), 7-29.

11. Dinev, T. & Hart, P. (2006b). Privacy Concerns and Levels of Information Exchange: An Empirical Investigation of Intended E-Service Use. *E-Service Journal*, 6 (1), 25-59.
12. Fletcher, K. (2003). Consumer Power and Privacy: The Changing Nature of CRM. *International Journal of Advertising*, 22, 249-272.
13. Gillmor, D. (1998). Violating Privacy is Bad Business. *Computerworld*, 32 (12), 38-39.
14. Graeff, T.R. & Harmon, S. (2002). Collecting and Using Personal Data: Consumers' Awareness and Concerns. *The Journal of Consumer Marketing*, 19, 302-318.
15. Hall, E.T. (1976). *Beyond Culture*. Garden City, NY: Anchor Press/Doubleday.
16. Hofstede, G. (1980). *Culture's Consequences: International Differences in Work-Related Values*. Beverly Hills, CA: Sage.
17. Hui, K., Teo, H., & Lee, S. T. (2007). The Value of Privacy Assurance: An Exploratory Field Experiment. *MIS Quarterly*, 31 (1), 19-33.
18. Keegan, W. & Green, M.C. (2008). *Global Marketing*. Upper Saddle River, N.J.: Pearson Prentice Hall.
19. Milne, G.R. & Boza, M. (1999). Trust and Concern in Consumers' Perceptions of Marketing Information Management Practices. *Journal of Interactive Marketing*, 13, 5-24.
20. Miyazaki, A.D. & Krishnamurthy, S. (2002). Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions. *The Journal of Consumer Affairs*, 36, 28-49.
21. Nam, C., Song, C., Lee, E., & Park, C. (2006). Consumers' Privacy Concerns and Willingness to Provide Marketing-Related Personal Information Online. *Advances in Consumer Research*, 33, 212-217.
22. Nijhawan, D.R. (2003). The Emperor Has No Clothes: A Critique of Applying the European Union Approach to Privacy Regulation in the United States. *Vanderbilt Law Review*, 56 (3), 939-976.
23. Papazafeiropoulou, A. & Pouloudi, A. (2001). Social Issues in Electronic Commerce: Implications for Policy Makers. *Information Resources Management Journal*, 14 (4), 24-32.
24. Raab, C.D. & Bennet, C.J. (1998). The Distribution of Privacy Risks: Who Needs Protection? *The Information Society*, 14 (4), 253-262.
25. Rice, R.E., McCreadie, M., & Chang, S.L. (2001). *Accessing and Browsing Information and Communication*. Cambridge, MA: The MIT Press.
26. Rindfleish, T.C. (1997). Privacy, Information Technology, and Healthcare. *Communications of the ACM*, 40, 92-100.
27. Rust, R.T., Kannan, P.K., & Peng, N. (2002). The Customer Economics of Internet Privacy. *Journal of the Academy of Marketing Science*, 30, 455-464.
28. Saunders, K. & Zucker, B. (1999). Contracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act. *International Review of Law, Computers, and Technology*, 13 (2), 183-192.
29. Sheehan, K.B. & Hoy, M.G. (2000). Dimensions of Privacy Concern Among Online Consumers. *Journal of Public Policy and Marketing*, 19 (1), 62-73.
30. Spiekermann, S., Grossklags, J., & Berendt, B. (2001). E-Privacy in 2nd Generation E-Commerce. Privacy Preferences versus Actual Behavior. In Proceedings of EC'01: Third ACM Conference on Electronic Commerce. New York: Association for Computing Machinery, 38-47.
31. Staples, B. (2004). The Battle Against Junk Mail and Spyware on the Web. *New York Times*, January 3.
32. Strauss, J., El-Ansary, A., & Frost, R. (2006). *E-Marketing*. Upper Saddle River, NJ: Pearson Prentice Hall.
33. Wang, H., Lee, M.K.O., & Wang, C. (1998). Consumer Privacy Concerns About Internet Marketing. *Communications of the ACM*, 41, 63-70.