Predicting Consumer Reaction To Online Privacy Concerns: A Nested Logit Model

Soumava Bandyopadhyay, Ph.D., Lamar University, USA

ABSTRACT

This paper proposes a theoretical choice model to explain how consumers may react to their concerns regarding online information privacy. A nested logit model is suggested as the appropriate model to predict the choice of online privacy risk management strategies by consumers. Conceptual justification is provided for the proposed model. The validity of the major assumptions behind the model in the context of Internet use is explained. Managerial implications and future research directions are also discussed.

Keywords: Online Information Privacy; e-Commerce; Consumer Reaction; Nested Logit Model

INTRODUCTION

With the phenomenal growth of Internet usage and e-commerce, there is a growing concern about online privacy protection. Invasion of online privacy involves the unauthorized collection, disclosure, or other use of personal information (Wills and Zeljkovic, 2011; Wang, Lee, and Wang, 1998). Personal information is often asked for when consumers are required to register at web sites before being able to browse free content. It is virtually impossible for consumers to transact business online without revealing personal information (Rust, Kannan, and Peng, 2002). In addition, consumers' personal information could be obtained involuntarily by the use of cookies that track people's online surfing behavior (Pierson and Heyman, 2011). Vast amounts of information can be thus collected over the Internet, and digital networks can link all this private information in databases (Caruso, 1998). This information can then be bought, sold, and traded, possibly without the consumers' permission, which increases consumers' concerns regarding having to reveal personal information online, and regarding the way in which such information might be used (Yao, Rice and Wallis, 2007; Ohm, 2010; Fletcher, 2003). Such concerns range from the intrusion of one's privacy and being targeted with unsolicited advertisements, to potential hassles resulting from online identity theft. If Internet users get increasingly concerned about online privacy, the fallout could range from consumers declining to provide personal information online, or provide false information, to the outright rejection of e-commerce, or even minimizing the use of the Internet (Nam et al., 2006; Dinev and Hart, 2006a; Wills and Zeljkovic, 2011). What consumers will actually do in reaction to their concern for online information privacy will depend upon what kind of online privacy risk management strategy they would like to pursue.

This paper proposes a theoretical choice model of risk-management strategy use by consumers concerned with online information privacy. Empirical testing of the proposed model, and future research possibilities are also discussed.

CLASSIFYING ONLINE PRIVACY RISK MANAGEMENT STRATEGIES

Consumers perceive a risk when they are concerned about online information privacy. To treat this risk, consumers will seek to pursue an appropriate risk management strategy. ISO/IEC 27002 is an international standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), which includes guidelines and general principles for managing information security in an organization (*International Organization for Standardization*, 2007). According to this standard, there are four alternative approaches to risk management: 1) *risk avoidance*, where risk is avoided by not performing a potentially risky activity at all; 2) *risk mitigation*, where risk is reduced through countermeasures; 3) *risk acceptance*, where nothing is done to reduce risk; and 4) *risk transference*, where the risk is transferred to third parties, such as insurers. In the context of consumer use of risk management strategies for personal Internet usage, the risk transference strategy will not be applicable. So, we assume that three main categories of risk management strategies would be used by consumers concerned about online information privacy: risk avoidance, risk mitigation, and risk acceptance.

After selecting a broad category of risk management strategy, consumers will have to decide what specific risk treatment method within the category should be pursued. A survey of the online information privacy literature suggests that several options are available and are used by consumers. These are outlined next.

Risk Avoidance strategies

In this category, any online activity that puts the consumer at risk of compromising personal information will be minimized, or avoided altogether. The following are possible:

- The consumer will avoid using web sites that require personal information before allowing the use of content (Rice, McCreadie, and Chang, 2001).
- The consumer will not conduct sales transactions at e-commerce sites that require online divulgence of credit card and other identifiable information (Graeff and Harmon, 2002).
- The consumer will avoid using the Internet altogether because of the fear that personal information can be automatically collected by web sites (through cookies and/or spyware) without the consumer’s knowledge or permission (Nam et al., 2006)

Risk Mitigation strategies

Here, the consumer will use the Internet, but will adopt specific countermeasures to alleviate the risk of compromising personal information. This is a proactive approach. The following possibilities exist under this category:

- The consumer will try to control the unauthorized collection of private data online by taking measures such as installing anti-virus and anti-spyware software, setting the browser’s privacy and security options appropriately, or scrutinizing the posted privacy policy of the web site (Spiekermann, Grossklags, and Berendt, 2001, Tsai et al., 2011).
- The consumer will provide false information if a web site requires registration with personal information before letting someone use its content (Dinev and Hart, 2006b).
- The consumer will conduct an e-commerce transaction at a web site only if the site accepts a payment method other than providing credit card information online, such as pay by phone, mail, or at a store (Graeff and Harmon, 2002).

Risk Acceptance strategies

This is a passive approach to managing risk, where the consumer continues to use the Internet as usual, hoping that unauthorized collection and subsequent misuse of personal information will not take place. The following options are possible under this category:

- The consumer will not adopt any protective technological measures (adjusting the browser’s privacy and security settings, installing anti-spyware software, etc.) to alleviate data privacy risks, and will continue to browse the Web as usual (Alreck and Settle, 2007).
- The consumer will provide personal information to web sites if required to do so as a precondition to using the site’s content (Alreck and Settle, 2007).
- The consumer will provide credit card and other personal information while shopping online (Alreck and Settle, 2007).

It is seen that the decision to apply a particular risk management strategy follows a hierarchical model of choice. The consumer first chooses a type of risk management approach (avoidance, mitigation, or acceptance), and then chooses a specific strategy under that broad category. The decision hierarchy is illustrated in Figure 1.

Figure 1
Decision Hierarchy for Consumer Online Information Privacy Risk Management Strategies

Online Privacy Risk Management Strategies

Risk Avoidance
- Avoid web sites that require information
- Avoid e-commerce transactions
- Avoid using Internet

Risk Mitigation
- Install protective software, etc.
- Provide false personal information
- Conduct transaction only if online credit card info not required

Risk Acceptance
- Use Internet without protective measures
- Provide personal information to web sites
- Provide credit card information for online shopping

A CHOICE MODEL FOR CONSUMER ONLINE PRIVACY RISK MANAGEMENT

Stochastic choice models have been extensively used in consumer behavior research. In these models, researchers assume that each member of a population purchases according to a given probability of purchase model, but that these individuals vary in terms of their lifestyles, past purchase behavior, level of involvement, and so on (Lilien, Kotler, and Moorthy, 1992). The probability of purchase also varies according to the context of the purchase situation. Similar assumptions can be made in modeling the consumer’s process of managing online privacy risk. There will be a certain probability behind the choice of any risk management strategy depending on the characteristics of the consumer, such as awareness of online information privacy issues, level of concern about online privacy, level of risk tolerance, ability (i.e., technical expertise) to control unauthorized collection and misuse of personal information, etc. (Dinev and Hart, 2004, 2006a; Culnan and Armstrong, 1999, Schwartz and Solove, 2011). Also, the context of Internet use is likely to influence the choice of risk management strategy. For example, consumers are more likely to choose risk acceptance if a web site posts a comprehensive privacy policy, and risk avoidance in the absence of such a policy (Tsai et al., 2011). A risk mitigation strategy is likely when the consumer is uncertain about the privacy policy of a web site, but is still attracted to the site for its content or shopping offerings.

The most commonly applied model for hierarchical decision making in marketing is the nested logit model (Lilien, Kotler, and Moorthy, 1992). Following this model in consumer research, the consumer first chooses a product form and then selects a specific brand. Following the decision hierarchy for online information privacy risk management strategies shown in Figure 1, the consumer will first choose a broad strategy category (risk avoidance, risk mitigation, or risk acceptance), and then choose a specific strategy within that category. This suggests the application of the *nested logit model* to predict the risk management decision process. This model is explained in the next section.

THE NESTED LOGIT MODEL

The nested logit model (Ben-Akiva and Lerman, 1985; Lilien, Kotler, and Moorthy, 1992) is a modified version of the multinomial logit model (Malhotra, 1984; Batsell and Lodish, 1981; Gensch, 1985), following which a consumer would choose an information privacy risk management strategy to provide the maximum utility. The utility is measured by the extent to which the strategy is able to alleviate the risk of unauthorized collection and use of personal information online. The utility would be reduced if, in a given situation, the strategy fails to alleviate such risk. The choice mechanism of the risk management strategy is deterministic, as the consumer chooses a strategy based on his/her own perceptions of vulnerability to risk, negative outcomes of compromising personal information, ability to control unauthorized information collection and use, etc. The utility of the risk management strategies, however, undergoes random fluctuations as different results are sometimes obtained from applying the same strategy. For example, unprotected Internet surfing (risk acceptance) may result in unauthorized personal data collection on some occasions, but not on others. Thus, the choice of risk management strategies follows the assumptions of random utility, deterministic choice mechanism, and utility maximizing behavior. These assumptions justify the use of the multinomial logit model.

There is, however, one problem with the multinomial logit model being applied to hierarchical decisions such as choice of risk management strategies. This is the assumption of Independence of Irrelevant Alternatives (commonly called the IIA assumption), which states that the relative odds of two alternatives are independent of the attributes of a third alternative (Malhotra, 1984). The IIA assumption is not likely to be satisfied in the hierarchical choice model for consumer online privacy risk management strategies. Suppose the choice set consists of one risk avoidance strategy, to avoid browsing web sites that ask for personal information, and one risk mitigation strategy, to provide false information when a web site asks for personal information as a precondition to using its content, both with the same utility so that they have equal probability (.5) of being chosen. Now, if another risk mitigation strategy, to install protective software to prevent the unauthorized collection of software, becomes available to the consumer having the same utility as the "providing false information" strategy, then, under the IIA assumption, all three strategies will still have an equal probability (.33) of being chosen. This is obviously unrealistic. Since different categories of risk management strategies are available, it is more likely that the newly available strategy to install protective software will be used more at the expense of providing false information (the other risk mitigation strategy) than at the expense of the strategy to avoid browsing web sites that ask for personal information, which belongs to another category (risk avoidance).

The nested logit model overcomes the problem of the IIA assumption by relaxing it in a hierarchical decision-making situation (Dubin, 1986; Lilien, Kotler and Moorthy, 1992). It is assumed that the utility that is common to all categories of risk management strategies and the utility associated with specific risk management strategies can be identified. Then, we have:

$$U_{xy} = U_x + U_{y\backslash x} \tag{1}$$

where:

U_{xy} = utility from choosing category of risk management strategy *x* and specific strategy *y*
U_x = utility associated with category of risk management strategy *x*
$U_{y\backslash x}$ = unique utility of risk management strategy *y* (under strategy category *x*)

For the probabilities of choosing risk management strategies in the hierarchical model, we may write:

$$P_{xy} = P_{y\backslash x} \,.\, P_x \tag{2}$$

where:

P_{xy} = probability of choosing risk management strategy *y* and strategy category *x*
P_x = unconditional probability of choosing strategy category *x*
$P_{y\backslash x}$ = probability of choosing risk management strategy *y*, given strategy category *x*

Following the standard derivation procedure for the nested logit model (Lilien, Kotler, and Moorthy, p.104), probability $P_{y\backslash x}$ is given as:

$$P_{y\backslash x} = \frac{\exp U_{y\backslash x}}{\Sigma_z \exp U_{z\backslash x}} \tag{3}$$

where there are z different risk management strategies available under strategy category x.

The equation for the strategy category probabilities is given by:

$$P_x = \frac{\exp \mu[U_x + \ln(\Sigma_y \exp U_{y\backslash x})]}{\Sigma_{x'} \exp \mu\{U_{x'} + \ln[\Sigma_y(\exp U_{y\backslash x'})]\}} \qquad (4)$$

where μ is a normalizing constant.

The probability of choosing risk management strategy y in strategy category x can be derived by substituting equations (3) and (4) into equation (2). Thus, we have the probability of choosing risk management strategy y in strategy category x as:

$$P_{xy} = \frac{\exp U_{y\backslash x}}{\Sigma_z \exp U_{z\backslash x}} \cdot \frac{\exp \mu[U_x + \ln(\Sigma_y \exp U_{y\backslash x})]}{\Sigma_{x'} \exp \mu\{U_{x'} + \ln[\Sigma_y(\exp U_{y\backslash x'})]\}} \qquad (5)$$

MODEL ESTIMATION

The theoretical choice model described in this paper needs to be validated by rigorous empirical testing. The estimation of the model calls for surveying consumers who use the Internet. The respondents in the survey are to be asked whether (0 = no, and 1 = yes) they use the nine strategies under the three categories (Figure 1) to manage their online information privacy risk. The 0/1 scheme is to be used since a nested logit model has to be estimated using a choice (0/1) response. Another option is to ask the respondents *how many times* (during the past year, six months, one month, or so) each of the nine strategies were used so as to obtain the aggregate frequency of use of each strategy, which is also acceptable in estimating a nested logit model (Lilien, Kotler, and Moorthy, 1992). Besides the frequency of use of the nine strategies under the three broad categories (risk avoidance, risk mitigation, and risk acceptance), the respondents would also be asked about their perceived utilities associated with each risk management strategy, i.e., whether each strategy is effective (0 = ineffective, 1 = effective) in obtaining the desired outcome, which is the lowering of online information privacy risk.

Aggregation of the data collected from all the respondents will provide the major predictor component of the nested logit model (see equation 5 in the previous section)—the utilities expected from the nine strategies. The data on the frequency of use of the various strategies relative to one another will provide the probability of use of each strategy. By substituting the numbers thus obtained for the probabilities and utilities in equation (5), one can estimate the normalizing constant μ. Once the normalizing constant is estimated, the model can be applied to predict the risk management strategy use by consumers.

MANAGERIAL IMPLICATIONS

The purpose of the model is to predict the online privacy risk management strategies that consumers will use. Obviously, marketers will want consumers to pursue certain strategies over others. For example, marketers would not want consumers to choose a risk avoidance strategy of not using web sites that ask for personal information, or of not participating in e-commerce transactions, or of limiting Internet use altogether. Marketers would also not want consumers to choose a risk mitigation strategy of providing false personal information to web sites, or of not using their credit cards for online transactions. If consumers are to pursue a risk mitigation strategy, marketers would prefer that they do so by installing software (e.g., firewalls, browser security fixes) or by following procedures such as setting browser configurations to prevent tracking cookies from being implanted without the user’s permission. These approaches will mitigate the risk of unauthorized personal information collection and use without the consumer having to limit Internet use or avoid e-commerce transactions. Marketers would also want consumers to choose a risk acceptance strategy more often, whereby consumers will more freely surf the Internet, provide truthful personal information (which can be used for legitimate marketing purposes). 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.

To convince the consumers to choose a risk acceptance strategy, marketers will have to make them perceive a greater utility from such a strategy, as per our nested logit model. Posting a comprehensive privacy policy on the web site should convince consumers regarding the procedural fairness in the collection and use of personal data, and increase consumers' trust in the web site (Culnan and Armstrong, 1999). When consumers trust a web site, they will perceive a lesser degree of vulnerability to risk from browsing, providing information, or engaging in e-commerce transactions (Tsai et al., 2011) and will feel that the benefits of accepting the risk will outweigh the cons.

FUTURE RESEARCH

Two major opportunities for fine-tuning the model's predictive power exist: 1) to include demographic characteristics of consumers; and 2) to estimate the model across diverse cultures. Demographic factors such as age, and gender have been known to influence consumer risk perception in Internet use and shopping behavior (Youn, 2009; Forsythe and Shi, 2003; Bhatnagar, Misra, and Rao, 2000). It will be useful to see how different demographic segments perceive different utilities for the online information privacy risk management strategies described in our model. The influence of national cultural characteristics on online privacy concerns has also been recognized (Bellman et al., 2004). The nested logit model described in this paper could be estimated in different countries to address the online information privacy risk issues across cultures.

CONCLUSION

In this paper, a nested logit model is proposed to predict how consumers may choose specific risk management strategies to address their concerns regarding online information privacy. The focus is on examining the appropriateness of the nested logit model given the hierarchical decision-making involved in the choice of an appropriate risk management strategy, rather than the mathematical derivation of the nested logit model itself, which has been adequately reported in the literature (Lilien, Kotler, and Moorthy, 1992; Malhotra, 1984; Dubin, 1986). It appears that the nested logit model is well-suited to predict the choice of online privacy risk management strategies and, consequently, to predict the relative use of the various available strategies. Methods to empirically test the proposed model are suggested, and future research directions are also outlined.

AUTHOR INFORMATION

Soumava Bandyopadhyay, Ph.D., is a professor of marketing at Lamar University, U.S.A. His areas of research interest include Internet-based marketing, global marketing, and channels of distribution. Contact: Lamar University, Department of Management and Marketing, P.O. Box 10025, Beaumont, TX 77710. E-mail: soumava.bandyopadhyay@lamar.edu

REFERENCES

1. Alreck, P.L. & Settle, R.B. (2007). Consumer Reactions to Online Behavioral Tracking and Targeting. *Journal of Database Marketing & Customer Strategy Management*, 15 (1), 11-23.
2. 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.
3. Batsell, R.R. & Lodish, L.M. (1981). A Model and Measurement Methodology for Predicting Individual Consumer Choice. *Journal of Marketing Research*, 18 (February), 1-12.
4. 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.
5. Ben-Akiva, M. & Lerman, S.R. (1985). *Discrete Choice Analysis: Theory and Application to Travel Demand*. Cambridge, MA: MIT Press.
6. Bhatnagar, A., Misra, S. & Rao, H.R. (2000). On Risk, Convenience, and Internet Shopping Behavior. *Communications of the ACM*, 43 (11), 98-105.

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. Dubin, J.A. (1986). A Nested Logit Model of Space and Water Heater System Choice. *Marketing Science*, 5 (2), 112-124.
13. Fletcher, K. (2003). Consumer Power and Privacy: The Changing Nature of CRM. *International Journal of Advertising*, 22, 249-272.
14. Forsythe, S.M. & Shi. B. (2003). Consumer Patronage and Risk Perceptions in Online Shopping. *Journal of Business Research*, 56 (11), 867-875.
15. Gensch, D.H. (1985). Empirically Testing a Disaggregate Choice Model for Segments. *Journal of Marketing Research*, 22 (November), 462-467.
16. Graeff, T.R. & Harmon, S. (2002). Collecting and Using Personal Data: Consumers' Awareness and Concerns. *The Journal of Consumer Marketing*, 19, 302-318.
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. International Organization for Standardization. (2007). *ISO/IEC 27002:2005 Information Technology – Security Techniques – Code of Practice for Information Security Management.* Geneva: ISO.
19. Lilien, G., Kotler, P. & Moorthy, K.S. (1992). *Marketing Models*. Englewood Cliffs, NJ: Prentice Hall.
20. Malhotra, N.K. (1984). The Use of Linear Logit Models in Marketing Research. *Journal of Marketing Research*, 21 (February), 20-31.
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. Ohm, P. (2010). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review*, 57, 1701-1777.
23. Pierson, J. & Heyman, R. (2011). Social Media and Cookies: Challenges for Online Privacy. *Info: The Journal of Policy, Regulation, and Strategy for Telecommunications*, *Information, and Media*, 13 (6), 30-42.
24. Rice, R.E., McCreadie, M., & Chang, S.L. (2001). *Accessing and Browsing Information and Communication*. Cambridge, MA: The MIT Press.
25. 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.
26. Schwartz, P.M. & Solove, D.J. (2011). The PII Problem: Privacy and a New Concept of Personally Identifiable Information. *New York University Law Review*, 86, 1815-1894.
27. 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.
28. Tsai, J.Y., Egelman, S., Cranor, L. & Acquisti, A. (2011). The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. *Information Systems Research*, 22 (2), 254-268.
29. Wang, H., Lee, M.K.O., & Wang, C. (1998). Consumer Privacy Concerns About Internet Marketing. *Communications of the ACM*, 41, 63-70.
30. Wills, C.E. & Zeljkovic, M. (2011). A Personalized Approach to Web Privacy: Awareness, Attitudes, and Actions. *Information Management & Computer Science*, 19 (1), 53-73.
31. Yao, M.Z., Rice, R.E. & Wallis, K. (2007). Predicting User Concerns About Online Privacy. *Journal of the American Society for Information Science and Technology*, 58 (5), 710-722.
32. Youn, S. (2009). Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents. *The Journal of Consumer Affairs*, 43 (3), 389-418.

NOTES