The current issue and full text archive of this journal is available at
www.emeraldinsight.com/0968-5227.htm



Received 27 July 2008
Revised 9 December 2008
Accepted 9 December 2008

# Consumer motivations in taking action against spyware: an empirical investigation

Anil Gurung
*Neumann University, Aston, Pennsylvania, USA*
Xin Luo
*Anderson School of Management, The University of New Mexico, Albuquerque, New Mexico, USA, and*
Qinyu Liao
*Department of Business Administration, School of Business, The University of Texas at Brownsville and Texas Southmost College, Brownsville, Texas, USA*

## Abstract

**Purpose** – The purpose of this paper is to develop a research framework and empirically analyze the factors that motivate the consumers to adopt and use anti-spyware tools when they are faced with security threats.

**Design/methodology/approach** – The research model was tested with data obtained through online survey questionnaires. A pre- and a pilot-test of the survey instrument are conducted. Then, a final five-point Likert scale instrument is created. The solicitation for participants is done through e-mail invitations. Survey results are analyzed using factor analysis and logistic regression.

**Findings** – The results do not find statistically significant relationships for hypotheses related to perceived vulnerability and response cost with the dependent variable. Perceived severity, self-efficacy, and response efficacy are significantly related to use of anti-spyware tools.

**Research limitations/implications** – The empirical findings suggest that protection motivation theory (PMT) may possibly provide a new avenue in the domain of IS adoption. In addition to the usefulness and ease of use in the classical IT adoption models, the threat appeal factors are added in this study to provide a different perspective in understanding technology adoption behavior.

**Practical implications** – The findings provide insights for business managers and information security professionals attempting to deliver to and implement security mechanisms like anti-spyware among end-users who are faced with security threats.

**Originality/value** – While theories such as technology acceptance model, theory of planned behavior and theory of reasoned action are insufficient to gauge consumers' attitude and behavioral change toward the adoption of anti-spyware tools when consumers are confronted with threats, this paper provides theoretical support and contributions to the research based on applying PMT in the arena of information systems.

**Keywords** Motivation (psychology), Consumer behaviour, Computer software, Data security

**Paper type** Research paper

Information Management & Computer Security
Vol. 17 No. 3, 2009
pp. 276-289

0968-5227
DOI 10.1108/09685220910978112

## Introduction

Classified as "the ghost in machine" (Stafford and Urbaczewski, 2004), spyware generally refers to a wide range of software that monitors computers usage without

a user's knowledge or consent. While most people regard spyware as a stealthy transmitter gathering and passing sensitive personal information to a third party over the internet, Warkentin *et al.* (2005) further expanded the description by defining spyware as a client-side software component that monitors the use of client activity and sends the collected data to a remote machine. Based on this definition with four distinct classes, this paper primarily focuses on the parasite aspect of spyware and conceives that the launch of vicious spyware mainly stems from the search for valuable information. In actuality, unlike most viruses which may destroy and modify other data, spyware is a subset of malware with distinct characteristics for data collection and transmission in a surreptitious fashion. Spyware tracks a user's online activities, triggers pop-up windows designed to lure online business, steals and records passwords, or even takes control of a user's computer. Additionally, spyware is able to trigger system resource misuse and bandwidth waste, thereby posing grave security, confidentiality, and compliance risks (Luo, 2006). As such, spyware exacerbates the privacy concerns of consumers due to its stealthy characteristics.

Spyware has grown to be an epidemic on the internet. According to the study published by AOL and National Cyber Security Alliance, 38 percent home computers lack any spyware protection software and 54 percent interviewed participants are unaware of the existence of spyware on their computers (AOL/NCSA, 2005). The threats related to spyware are more severe in the sense that its existence is not as obvious as the existence of viruses or worms. Unlike the direct attacks from viruses or worms, spyware installations can be authorized as a part of the licensed agreement that a user agrees to when downloading free utility and file sharing programs from the internet. In some cases, spyware is installed as a part of legitimate computer applications provided by business to their customers to provide updating and communicative functionality to application users (Stafford and Urbaczewski, 2004). Since spyware may be masqueraded and sometimes bundled with legitimate programs (Stafford and Urbaczewski, 2004), they appear to be a safe program and thus can circumvent the detection of antivirus applications. In addition, spyware writers are among the best and brightest programmers who are well compensated for their skills by illicit marketing firms (Davis, 2007). Apart from the legitimate business of spyware for marketing segmentation and audience targeting, there are many malicious uses. Known risks posed by spyware are: transmission of information of consumers, their computer and their surfing habits to third parties; remote hijacking to access, delete or even modify files; capture keystrokes of consumers to steal private or confidential information; and slow down computer performance due to wasteful consumption of bandwidth on personal computers (Thompson, 2005).

A recent US study revealed that over 90 percent of broadband users sampled had computer infected with spyware (Baig, 2004). Schmidt and Arnett (2005) found that users who know the nefarious effects of spyware may not necessarily know the specifics of how spyware is obtained or prevented. Even though spyware's aftermath varies from severe to mild (Warkentin *et al.*, 2005), not many consumers appear to have practically taken remedial actions to fight against the ghost in the machine. This abnormality can be explained by the fact that most of the time consumers are unaware that their machines have been infected by spyware (Luo, 2006) or they may consider their standard anti-virus software sufficient for spyware protection (Lee and Kozar, 2005). In addition to the inadequate skills and resources to take defensive actions for

the threat of spyware, Hu and Dinev (2005) found that lack of awareness is an important reason of not taking any action against spyware. Interestingly, the study by Poston *et al.* (2005) showed that only 45 percent of the respondents had installed and used spyware protection on their computers and that 74.9 percent of the respondents were aware of spyware. Thus, there is a clear indication that being aware of spyware does not necessarily lead to taking action against spyware. Recent studies by Warkentin *et al.* (2005) and Luo (2006) have proposed a spyware assessment model and a holistic approach for managing spyware. Motivation has also been suggested in an online customer privacy and identity protection framework (Milne *et al.*, 2004), yet little research has been done to scientifically investigate the motivation for consumers to use anti-spyware tools and those factors that lead to the adoption of anti-spyware tools for consumers. While endeavoring to bridge this gap, this study also attempts to discuss whether existing models of technology adoption are applicable to the adoption of spyware tools.

In this study, the motivation of consumers to adopt anti-spyware tools is explained by using the theoretical foundation of protection motivation theory (PMT) (Rogers, 1983). Non-adopters of anti-spyware tools may not be aware of the severity of risks caused by spyware. Awareness has been one of the important determinants in the adoption of anti-spyware tools (Hu and Dinev, 2005). Non-adopters may have been aware of existence of spyware but not completely cognizant of the degree of risks. Besides, they may not have the required skills to install and use anti-spyware tools. Given these intriguing artifacts, this study develops and empirically validates a research framework for the adoption of anti-spyware tools when consumers are faced with security threats. The rest of the paper is outlined as follows: an overview of the theoretical background is offered; the research model and hypotheses are presented; the methodology section describes how the model validation is conducted, followed by data results and analysis. The last section describes the implications and conclusions of this study.

## Theoretical background

There has been very limited empirical research in the area of spyware. Earlier works have used the theory of planned behavior (TPB) to predict the adoption of anti-spyware tool (Hu and Dinev, 2005; Lee and Kozar, 2005). Although the TPB has provided insights into the importance of factors such as attitude, social norms and perceived behavioral control in predicting the use of anti-spyware tools, we believe that additional factors may be significant in predicting the adoption of these tools. In situations where individuals are faced with fear or danger, it is known that their attitude and behavior may change. For example, in conditions where the web browser of a user's personal computer has been hijacked by a spyware, he/she is likely to search for anti-spyware tools to free he or she from the predicament at hand, although the anti-spyware tool may not have been used in his or her social circle or he/she may not have had a good attitude towards anti-spyware tools. The attitudinal-based theories such as the theory of reasoned action (TRA) (Ajzen and Fishbein, 1980) and the TPB (Ajzen, 1991) propose that attitudes are shaped by the beliefs regarding the outcomes associated with a behavior and attitudes, and in turn, influence the intention to perform a behavior and the behavior itself. Furthermore, these notions about attitude and behavior in the context of information technology are explained by the widely

acknowledged technology acceptance model (TAM) (Davis, 1989). However, as fear may change the attitude or behavior of individuals, attitudinal-based theories such as TAM, TRA, and TPB might have inadequacy in explaining the adoption of anti-spyware tools.

The PMT (Rogers, 1983), a viable theoretical framework in health and social psychology, provides a richer understanding of why attitudes and behavior can change when people are confronted with threats. Offering an important social cognitive account of diverse protective behavior, the PMT postulates that people tend to protect themselves from imminent danger or harm based on four types of cognitions or perceptions. These perceptions are the severity of the risks, vulnerability of risks, self-efficacy (SE) at performing the desired risk-reducing action, and the response efficacy (RE) of the desired behavior. The severity of risks refers to the perceptions of an individual regarding the magnitude of the consequences of threats. The vulnerability of risks refers to the likelihood that a threat would occur. The SE refers to one's capability to perform the protection behavior. The response-efficacy is one's judgment of how good would be the protection behavior. Information required for these cognitions comes from two sources: environmental and intrapersonal. The environment source of information may be verbal persuasion, and observational learning. Intrapersonal sources relates to prior experience. The theory further suggests that people would weigh the perceived costs and benefits of taking the desired protective behavior and would form their intentions to undertake the risk-reducing action based on their analysis.

These four analytical cognition processes may be grouped into the following sub-processes: threat and coping appraisal. Threat appraisal refers to the personal assessment of risks posed by the threat. A person goes through the threat appraisal by assessing the severity, vulnerability and benefits of taking the desired protection behavior. The other sub-process of coping appraisal refers to the personal assessment of one's ability to cope with or avoid the potential threat. The coping appraisal consists of SE, RE and costs related to taking the desired protection behavior. The SE refers to one's capability to perform the protection behavior. The response-efficacy is one's judgment of how good would be the protection behavior. The response cost (RC) is the summation of the costs related to money, time and effort that have to be borne if one has to perform the protection behavior. In essence, the main premise of the PMT is that protection motivation arises from the cognitive appraisal of a threat along with the belief that the desired protection behavior would effectively prevent the threat.

The threat in this research is related to the infection of the spyware on one's personal computer. Cumulatively, the combination of the threat and the coping appraisal processes activates a person's protective motivation, resulting in the applicable adaptive responses. The PMT has been validated in a diverse array of fields including health threats (i.e. smoking versus lung cancer), preventive behaviors, environmental hazards, protection of others, and adherence to medical treatment regimens (Floyd *et al.*, 2000). In the next section, we describe the research model and state the derived hypotheses.

## Research model and hypotheses

In this study, we adapt the PMT (Rogers, 1983) to predict the adoption of anti-spyware tools. The proposed research model is shown in Figure 1. The dependent variable of the

model is the use of anti-spyware tool which is a binary variable that determines the adopters and non-adopters. According to PMT, the threat appraisal is a process that evaluates the maladaptive behavior, which in this case is not adopting the anti-spyware tool. In the threat appraisal, the consumers will consider their perceptions about severity and vulnerability of the threats posed by spyware, and the intrinsic and extrinsic rewards of not adopting the protection measures. In this study, rewards are not included in the research model because we determine that the consumers will not get rewarded whatsoever for not using anti-spyware tools. The coping appraisal evaluates the ability to cope with and avert the threats of spyware. The factors that comprise the coping appraisal process are the two efficacy variables and the RC. RE is the belief that the protective measures will work or the adoption of anti-spyware tool will be effective in protecting against the threat of spyware. SE is the belief of an individual that he or she possesses the ability to conduct the protection measures or the use of anti-spyware tools. RC is the cost incurred in adopting the protective measures. These costs may include monetary resources, time and effort associated with using anti-spyware tools.

As shown in the research model, the processes of threat appraisal and coping appraisal would result in an outcome or personal decision of the consumer to initiate, continue or inhibit protective measures. By going through these two appraisal processes, consumers are likely to make a decision on the use of anti-spyware tools.

*Dependent variable*

The dependent variable of this research focuses on the behavior of consumers. The consumer's behavior towards anti-spyware use is an outcome of the processes of threat and coping appraisal. Some of the prior studies using PMT have studied the intentions (Rogers, 1975; Tanner *et al.*, 1991) while others studied the behaviors (Ho, 1998; Woon *et al.*, 2005). In this paper, we measure behavior because it is not very clear in the literature regarding the interaction of intention with cognition variables of PMT. Some previous research suggests two-way interactions and some others suggest three-way interactions between intention and cognition variables. Besides, there is also grounded support in the literature that intention is related with behavior, in line with expectancy-valence theory. Therefore, we tend to measure behavior in this study.

*Threat appraisal*

Threat appraisal is one of the processes that will mediate the effects of the components of fear appeals on attitudes by instigating protection motivation (Rogers, 1975). Threat appraisal evaluates the maladaptive behavior or the consequences of not using the

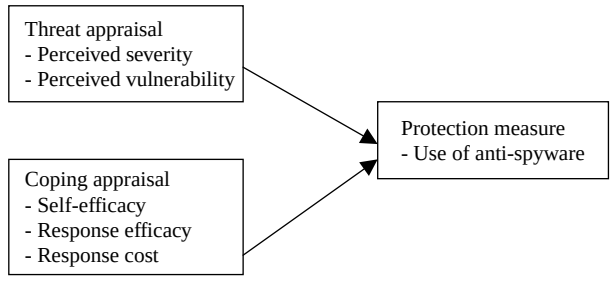


**Figure 1.**
Research model

anti-spyware tools in this study. As an intervening variable, protection motivation has the typical characteristics of a motive: it arouses, sustains, and directs a behavior (Rogers, 1975). It is assumed that protection motivation of consumers will arise from the cognitive appraisal of a spyware infection as noxious and likely to occur, along with the belief that the use of anti-spyware tools will effectively eliminate the occurrence of spyware infections. Perceived severity (PS) and perceived vulnerability (PV) are two threat appraisal constructs used in this study. PS refers to the perceptions of an individual regarding the magnitude of the consequences of a threat (Milne *et al.*, 2000). The consequences of spyware threat may relate to loss of personal or confidential information, slowdown of computer performance, etc. In consumer behavior literature, risk reduction strategies such as information seeking and brand loyalty are undertaken by consumers to lower the uncertainty associated with purchasing (Sheth and Venkatesan, 1968). The degree of risk is likely to increase when the PS is high. We thereby hypothesize that consumers are more likely to adopt risk-reduction behavior when the PS is high. Therefore, the first hypothesis is as follows:

*H1.* PS will have a positive relationship in determining that anti-spyware tool will be used.

According to Rogers (1983), PV or expectancy of exposure to threats refers to the likelihood of the occurrence of a threat. In our study, the threat refers to likelihood of occurrence of spyware infections. A significant relationship between PV and the coping response has been validated and reported (Rippetoe and Rogers, 1987). In the context of information systems for this research, consumers are more likely to use anti-spyware if they believe that they have a high chance of being negatively affected by spyware. Therefore, we hypothesize that:

*H2.* PV will have a positive relationship in determining the utilization of anti-spyware tools.

*Coping appraisal*

Coping appraisal process evaluates the ability to cope with and avoid threats (Floyd *et al.*, 2000). The factors related to the coping appraisal process are SE, RE, and RC. SE refers to an individual's capability in performing the desired behavior. In this study, the desired behavior is the use of anti-spyware tools. The significant relationship between SE and coping response has been reported in numbers of previous studies (Beck and Lund, 1981; Maddux and Stanley, 1983; Milne *et al.*, 2000). We therefore test the following hypothesis:

*H3.* SE will be significant in determining the use of anti-spyware tools.

RE is the belief that the use of anti-spyware tools will be effective in protecting against spyware. A positive correlation between RE and coping response has been found in the literature (Maddux and Stanley, 1983). Therefore, we hypothesize that:

*H4.* RE will be positively associated with use of anti-spyware tools.

RC refers to the costs incurred in taking the adaptive coping response of adopting the anti-spyware tools. Such costs may include the money and time spent to acquire and

update the anti-spyware tools as well as the inconvenience and interruption of computer use when running the anti-spyware tools. RCs in this study include the time taken to run the anti-spyware tool. The support for the RC and the coping response has been reported (Neuwirth *et al.*, 2000). Thus, we hypothesize that:

*H5.* RC will be significant in determining the use of anti-spyware tools.

## Methodology

The research model was tested with data obtained using online survey questionnaires. A pre-test of the survey instrument was conducted with two researchers for content validity. Further, a pilot test with 48 students was completed. Based on the results from pre-test and pilot test, a final five-point Likert scale instrument with 17 items was created, with 1 – strongly agree and 5 – strongly disagree. The items used in the survey can be found in Appendix. For the main study, we requested participation from undergraduates at three universities, two in the North East and one in the South. The sample was drawn from business undergraduate students attending a required class in business curriculum. The student sample was deemed suitable for this research because this study relates to studying the use of anti-spyware tools and the students represent an appropriate group of users who are active in the world wide web. The solicitation was done through e-mail invitations. Those agreed to participate in the survey were requested to proceed to the web survey through a link in the e-mail.

Out of approximately 300 students contacted through e-mail, 251 agreed to participate in the survey. The survey was completely voluntary and the respondents could leave the web survey at any time. Of the 251 responses, 19 were discarded for incompleteness, thus leaving 232 for final data analysis. Before proceeding with data analysis, any identifying information of the respondents such as IP addresses and geographic regions were deleted. The sample consisted of 47.8 percent male and 52.2 percent female. As for the internet experience, 10.8 percent reported having less than 1 year, 32.8 percent between 1 and 3 years, 22.4 percent between 3 and 5 years, and 34.1 percent more than five years.

## Data analysis and results

The measurement model was evaluated for reliability and validity. The construct reliability was assessed by examining the cronbach's $\alpha$ values. As shown in Table I, all the values are well above the accepted level of 0.7 suggested by Nunnally (1978). The convergent and discriminant validity were assessed by factor analysis. Principal component analysis with varimax rotation was used. The results showed that all item loadings were above 0.5 and loaded strongly with their respective constructs, thus showing there is adequate convergent validity. Discriminant validity is ascertained

| Factor | Cronbach's $\alpha$ |
|---|---|
| PS (three items) | 0.854 |
| PV (three items) | 0.891 |
| SE (three items) | 0.893 |
| RE (four items) | 0.880 |
| RC (four items) | 0.838 |

**Table I.**
Item reliability

when each item loads strongly with its related construct than with any other constructs. As shown in Table II, all the items have adequate convergent and discriminant validity.

Logistic regression was used to test the research model. Since the dependent variable in our research model was adoption or non-adoption of anti-spyware software, logistic regression is preferred over multiple regression. Using a dichotomous dependent variable in multiple regression model violates the assumptions for hypothesis testing. Logistic regression is preferred over discriminate analysis when the dependent variable has two groups because the logistic regression appears more robust in situations where assumptions are not met (Hair *et al.*, 2002).

The relationship between the dependent variable and the independent variables was assessed based on the statistical significance of the final model as shown in Table III. The goodness-of-fit statistic ($\chi^2 = 33.531$, significance = 0.00) indicates that the logistic regression model is not significantly different from a perfect model that will correctly classify all respondents into groups. Exp (*B*) ratio determines the odd ratio that is associated with a particular outcome. Table IV shows that, SE has the highest odds ratio while PS has the lowest odds ratio of a non-adoptive person adopting anti-spyware tools.

The significance of the regression coefficients of the hypothesized independent variables was tested to find support for the proposed hypotheses. Wald statistics were used for testing the significance of the proposed hypotheses. The results are shown in Table IV. All factors except "perceived vulnerability" and "response cost" had coefficients significantly different from 0 ($p < 0.05$). Therefore, the second hypothesis

| | PV | RC | PS | SE | RE |
|---|---|---|---|---|---|
| PS1 | 0.096 | −0.053 | *0.766* | 0.100 | 0.085 |
| PS2 | 0.193 | −0.003 | *0.829* | 0.009 | −0.056 |
| PS3 | 0.162 | −0.051 | *0.796* | 0.080 | 0.137 |
| PV1 | *0.675* | 0.054 | 0.316 | 0.079 | 0.111 |
| PV2 | *0.787* | 0.078 | 0.266 | −0.037 | 0.161 |
| PV3 | *0.781* | 0.104 | 0.040 | 0.049 | 0.105 |
| SE1 | 0.033 | −0.076 | 0.088 | *0.885* | 0.090 |
| SE2 | −0.007 | −0.080 | 0.153 | *0.872* | 0.141 |
| SE3 | 0.074 | 0.039 | 0.006 | *0.789* | 0.164 |
| RE1 | 0.029 | 0.141 | 0.180 | 0.035 | *0.805* |
| RE2 | −0.006 | −0.066 | 0.137 | 0.173 | *0.759* |
| RE3 | 0.229 | 0.065 | −0.158 | 0.304 | *0.546* |
| RE4 | 0.236 | 0.077 | −0.031 | 0.094 | *0.608* |
| RC1 | 0.077 | *0.631* | −0.053 | 0.093 | 0.237 |
| RC2 | 0.075 | *0.796* | 0.068 | −0.045 | 0.089 |
| RC3 | 0.025 | *0.827* | −0.036 | −0.028 | −0.059 |
| RC4 | 0.186 | *0.764* | −0.079 | −0.120 | −0.050 |

**Table II.**
Factor analysis results

| Model | −2 Log likelihood | $\chi^2$ | df | Sig. |
|---|---|---|---|---|
| Final | 283.661 | 33.531 | 5 | 0.00 |

**Table III.**
Measures of model fit

that postulated "perceived vulnerability will have a positive relationship in determining that anti-spyware tools will be used" was not supported. Additionally, the fifth hypothesis that postulates "response costs will be significant in determining the use of anti-spyware tools" was also not supported. A summary of hypothesis tests is presented in Table V.

Further, the model was assessed for its discriminating power. In the sample, there were 132 adopters and 100 non-adopters of anti-spyware tools. The utility of the model is assessed by comparing the predicted group membership (i.e. Table VI) to known membership (i.e. Table VII). In order to determine that our model is useful the

| Behavior | | *B* | SE | Wald | df | Sig. | Exp(*B*) |
|---|---|---|---|---|---|---|---|
| Not use | PS* | 0.125 | 0.226 | 3.528 | 1 | 0.040 | 0.654 |
| | PV | 0.159 | 0.213 | 0.555 | 1 | 0.456 | 1.172 |
| | SE* | 0.778 | 0.178 | 19.056 | 1 | 0.000 | 2.177 |
| | RC | −0.241 | 0.212 | 1.288 | 1 | 0.256 | 0.786 |
| | RE* | 0.188 | 0.284 | 4.862 | 1 | 0.021 | 1.473 |
| | Constant | −2.010 | 0.824 | 5.955 | 1 | 0.015 | 0.134 |

**Table IV.** Results of logistic regression analysis

**Notes:** *$p < 0.05$; reference category – enabled group

| Hypothesis | Significance | Result |
|---|---|---|
| *H1.* PS will have a positive relationship in determining that anti-spyware tool will be used | 0.04 | Supported |
| *H2.* PV will have a positive relationship in determining that anti-spyware tool will be used | 0.456 | Not supported |
| *H3.* SE will be significant in determining the use of anti-spyware tool | 0.000 | Supported |
| *H4.* RE will be positively associated with the use of anti-spyware tool | 0.021 | Supported |
| *H5.* RC will be significant in determining the use of anti-spyware tool | 0.256 | Not supported |

**Table V.** Hypothesis test results

| | | Predicted | |
|---|---|---|---|
| Observed | Use | Not use | Percentage correct |
| Use | 107 | 25 | 81.1 |
| Not use | 51 | 49 | 49.0 |
| Overall percentage | 68.1 | 31.9 | 67.2 |

**Table VI.** Classification results

| | Predicted *N* | Marginal (%) |
|---|---|---|
| *Behavior* | | |
| Use | 132 | 56.9 |
| Not use | 100 | 43.1 |
| Valid | 232 | 100 |

**Table VII.** Case processing summary

classification rate of 67.2 percent, obtained from Table VI, has to exceed the chance accuracy rate by 25 percent (Hand *et al.*, 2001). The minimal model acceptance rate is calculated to be 0.636 ( $= (0.569^2 + 0.431^2)^*1.25$). Since the classification rate of 67.2 percent is greater than the minimal model acceptance rate, there is no reason to doubt the utility of our logistic regression model.

## Discussion

Our results did not find significant relationships for hypotheses related to PV and RC with the dependent variable. This suggests that although a person may feel vulnerable to spyware infection, he or she may not adopt anti-spyware tools. One way of explaining this result could be the lack of knowledge in using anti-spyware tools. Owing to the invisible feature of spyware, even if consumers are aware of their risks from spyware attacks, they need to acquire necessary skills first and probably be trained before they can use those anti-spyware tools to protect themselves. This is confirmed by the support for *H3* where SE is significantly related to anti-spyware use.

PS is found significant in determining anti-spyware use. Studies indicated that anti-spyware usefulness perception, users' perceived technical skills and lack of severity recognition can all influence its adoption (Lee and Kozar, 2005; Poston *et al.*, 2005). Awareness of the risks of spyware can be raised by consumer education. Once consumers understand the severity of spyware damage, they are more likely to take precautionary action such as using anti-spyware tools and complying with computer security policies.

Cost was found to be a hurdle for anti-spyware adoption especially when the threat of spyware is unrecognized and underestimated (Poston *et al.*, 2005). Therefore, the level of anti-spyware adoption may be different from other security tools that are bundled free with new systems. It has been suggested that multiple trial options as well as bundling of multiple protection systems can be used to improve anti-spyware adoption (Lee and Kozar, 2005). However, the finding about the relationship between RC and anti-spyware use in this study is insignificant. The explanation may be the widely available free anti-spyware tools such as Spybot, Lavasoft ad-aware, and Yahoo Antispy. Current anti-spyware prices range from those offered as freeware to hundreds of dollars. Many companies also offer time-limited free evaluation copies. Most personal computer users would choose a free version over a more expensive one. Although the cheaper or even free copies may not provide more powerful extras of the paid products, each anti-spyware is effective to a certain extent only. As the spyware gets more complex and advanced, new anti-spyware tools have to be developed to fix them.

As hypothesized, the positive associations between RE and the use of anti-spyware tools were confirmed by the data analysis. With the extensive use of internet and the long list of anti-spyware tools available in the market, customers would adopt the anti-spyware tools that proved to be effective. That is why anti-spyware companies offer free evaluation versions of their anti-spyware products as a marketing tool to attract existing and potential customers. The companies recognize that if customers like their products, they will possibly pay the premium to upgrade the software and probably recommend it to their networks such as organizations or social contacts to buy the more expensive professional versions.

## Implications for research and practice

The validated model provides some support for PMT in the arena of information systems. Although PMT has been widely used in marketing and health research, there has been few studies in information systems (IS) literature. We hope that PMT provides a possibly new avenue in the domain of IS adoption. In addition to the usefulness and ease of use in the classical IT adoption models, the threat appeal factors were added in this study to provide a different perspective in understanding technology adoption behavior. Undoubtedly, this is not at all a comprehensive model for studying anti-spyware use motivation. More factors including experience, peer influence, and technical support can be included for a more exhaustive model in future studies.

With the evolving spyware technology and increasing complexity of online advertising, anti-spyware effort is the price customers have to pay for the convenience of today's powerful computers and networks. With the increased awareness of the severity of spyware attacks through consumer education, they would be more likely to follow recommended protective measures and use anti-spyware tools. This should be accompanied by necessary anti-spyware training, especially when more and more fake anti-spyware surface to take advantage of growing public fear, so that users can have the adequate skills to utilize the protection tools.

## Conclusion

Proliferation of spyware offer new threats and challenges for the consumers and the online companies that endeavor to attract prospective consumers. Privacy concerns are expected to fuel the growth in spyware complexity. It is imperative that the online advertising industry find a way to balance the benefits and burdens it creates for society. The war against spyware is going to be a challenge in many respects involving multiple governments, legislative action and business communities. The adoption of anti-spyware tools will help alleviate the fears of consumers to some extent. This study found that PS, SE, and RE can motivate consumers, who face the threat of spyware infections, to adopt anti-spyware tools and provide partial support for the research model based on PMT. Future studies engaging more contributing factors are needed to provide better understanding of consumer anti-spyware usage.

## References

Ajzen, I. (1991), "The theory of planned behaviour", *Organizational Behavior and Human Decision Processes*, Vol. 50 No. 2, pp. 179-211.

Ajzen, I. and Fishbein, M. (1980), *Understanding Attitudes and Predicting Social Behavior*, Prentice-Hall, Englewood Cliffs, NJ.

AOL/NCSA (2005), "AOL/NCSA online safety study", available at: www.staysafeonline.info/pdf/safety_study_2005.pdf

Baig, E.C. (2004), "Keep Spies From Skulking into Your PC", *USA Today Online*, available at: www.usatoday.com/money/industries/technology/2004-01-22-spy_x.htm

Beck, K.H. and Lund, A.K. (1981), "The effects of health threat seriousness and personal efficacy upon intentions and behaviour", *Journal of Applied Social Psychology*, Vol. 11 No. 5, pp. 401-15.

Davis, F.D. (1989), "Perceived usefulness, perceived ease of use, and user acceptance of information technology", *MIS Quarterly*, Vol. 13 No. 3, pp. 319-40.

Davis, J.P. (2007), "Spyware protection", *Journal of Accountancy*, Vol. 203 No. 4.

Floyd, D.L., Prentice-Dunn, S. and Rogers, R.W. (2000), "A meta-analysis of research on protection motivation theory", *Journal of Applied Social Psychology*, Vol. 30 No. 2, pp. 407-29.

Hair, J.F., Tatham, R.L. and Anderson, R.E. (2002), *Multivariate Data Analysis*, 6th ed., Prentice-Hall PTR, Upper Saddle River, NJ, p. 1 v.

Hand, D., Mannila, H. and Smyth, P. (2001), *Principles of Data Mining*, MIT Press, Cambridge, MA.

Ho, R. (1998), "The intention to give up smoking: disease versus social dimensions", *Journal of Social Psychology*, Vol. 138 No. 3, pp. 368-80.

Hu, Q. and Dinev, T. (2005), "Is spyware an internet nuisance or public menace?", *Communications of the ACM*, Vol. 48 No. 8, pp. 61-6.

Lee, Y. and Kozar, K.A. (2005), "Investigating factors affecting the adoption of anti-spyware systems", *Communications of the ACM*, Vol. 48 No. 8, pp. 72-7.

Luo, X. (2006), "A holistic approach for managing spyware", *Information Systems Security*, Vol. 15 No. 2.

Maddux, J.E. and Stanley, M. (1983), "Protection motivation theory and self efficacy: a revised theory of fear appeals and attitude change", *Journal of Experimental Social Psychology*, Vol. 19, pp. 469-79.

Milne, G.R., Rohm, A.J. and Bahl, S. (2004), "Consumers' protection of online privacy and identity", *The Journal of Consumer Affairs*, Vol. 38 No. 2, pp. 217-32.

Milne, S., Sheeran, P. and Orbell, S. (2000), "Prediction and intervention in health-related behavior: a meta-analytic review of protection motivation theory", *Journal of Applied Social Psychology*, Vol. 30 No. 1, pp. 106-43.

Neuwirth, K., Dunwoody, S. and Griffin, R.J. (2000), "Protection motivation and risk communication", *Risk Analysis*, Vol. 20 No. 5, pp. 721-34.

Nunnally, J. (1978), *Psychometric Theory*, 2nd ed., McGraw-Hill, New York, NY.

Poston, R., Stafford, T.F. and Hennington, A. (2005), "Spyware: a view from the (online) street", *Communications of the ACM*, Vol. 48 No. 8, pp. 96-9.

Rippetoe, S. and Rogers, R.W. (1987), "Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat", *Journal of Personality and Social Psychology*, Vol. 52 No. 3, pp. 596-604.

Rogers, R.W. (1975), "A protection motivation theory of fear appeals and attitude change", *Journal of Psychology*, Vol. 91, pp. 93-114.

Rogers, R.W. (1983), "Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation theory", in Cacioppo, J. and Petty, R. (Eds), *Social Psychophysiology*, Guilford, New York, NY, pp. 153-76.

Schmidt, M.B. and Arnett, K.P. (2005), "Spyware: a little knowledge is a wonderful thing", *Communications of the ACM*, Vol. 48 No. 8, pp. 67-70.

Sheth, J.N. and Venkatesan, M. (1968), "Risk-reduction processes in repetitive consumer behaviour", *Journal of Marketing Research*, Vol. 5 No. 3, pp. 307-10.

Stafford, T.F. and Urbaczewski, A. (2004), "Spyware: the ghost in the machine", *Communications of the Association for Information Systems*, Vol. 14, pp. 291-306.

Tanner, J.F., Hunt, J.B. and Eppright, D.R. (1991), "The protection motivation model: a normative model of fear appeals", *Journal of Marketing*, Vol. 55, pp. 36-45.

Thompson, R. (2005), "Why spyware poses multiple threats to security", *Communications of the ACM.*, Vol. 48 No. 8, pp. 41-3.

Warkentin, M., Luo, X. and Templeton, G.F. (2005), "A framework for spyware assessment", *Communications of the ACM.*, Vol. 48 No. 8, pp. 79-84.

Woon, I.M.Y., Tan, G.W. and Low, R.T. (2005), "A protection motivation theory approach to home wireless security", paper presented at 26th International Conference on Information Systems, Las Vegas, NV.

## Appendix

*Perceived severity*

*PS1.* Sending out my personal information by spyware without my approval is a serious problem for me.

*PS2.* Slow down of my personal computer's performance is a serious problem for me.

*PS3.* Anonymous tracking of my online activities is a serious problem for me.

*Perceived vulnerability*

*PV1.* I feel that I could be a target of spyware infection when I browse the internet.

*PV2.* I am concerned that my personal computer will be attacked by spyware when I browse the internet.

*PV3.* I am vulnerable to the possible danger posed by spyware.

*Self-efficacy*

*SE1.* I am capable of installing anti-spyware tools.

*SE2.* Using anti-spyware tools is easy for me.

*SE3.* I could use anti-spyware tools if there was no one around to guide me as I go along.

*Response efficacy*

*RE1.* Employing anti-spyware tools will prevent the unauthorized release of my personal information.

*RE2.* Employing anti-spyware tools is an effective way to deal with spyware.

*RE3.* Employing anti-spyware tools will prevent the unnecessary slow down of my personal computer's performance.

*RE4.* Employing anti-spyware tools will help stop frequent pop-ups when I browse the internet.

*Response cost*

*RC1.* The cost of employing anti-spyware tools decreases the benefits achieved from them.

*RC2.* There are too many overheads associated with employing anti-spyware tools.

*RC3.* Employing anti-spyware tools would require a considerable investment of effort other than time.

*RC4.* Employing anti-spyware tools would be time consuming.

*Use*

USE1. Do you use any anti-spyware tools?

___Yes ___ No

**Corresponding author**
Xin Luo can be contacted at: luo@mgt.unm.edu