

USER PERCEPTIONS OF SOFTWARE WITH EMBEDDED SPYWARE: AN EMPIRICAL EVALUATION

Janice C. Sipior, College of Commerce & Finance, Villanova University, USA
janice.sipior@villanova.edu

Burke T. Ward, College of Commerce & Finance, Villanova University, USA
burke.ward@villanova.edu

Abstract

A research model and hypotheses explore software user perceptions of privacy, trust, and legal protection in using application software with embedded spyware. Empirical results reveal actual users of software with spyware, versus users of software without spyware, have lower trust perceptions of a software vendor. Further examination of trustworthiness as a multi-dimensional construct, reveals trustworthiness-ability and trustworthiness-integrity are important influences of overall trust of a vendor. The results may provide guidance to software vendors and government regulatory agencies in addressing the concerns associated with spyware.

Keywords: spyware, trust, privacy, legal protection.

1 INTRODUCTION

As an emerging topic, spyware is not yet well understood (Zhang 2005). The purpose of this paper is to propose a research model and hypotheses to explore user perceptions of privacy, trust, and legal protection in the use of application software within which spyware is embedded. We first review previous research on spyware to identify the focus of this research. Next, we discuss the theoretical foundations for our research model and hypotheses. We undertake an exploratory study to test our model of users' perceptions, of trust, privacy, and legal protection, resulting from actual use of legitimate application software with embedded spyware.

The empirical results indicate actual users of application software within which spyware is embedded, versus users of software with no spyware, perceive the trustworthiness and overall trust of a software vendor to be lower. Further examination of trustworthiness as a multi-dimensional construct, revealed the vendor's trustworthiness-ability, that is, competence and knowledge about the appropriate use of private user information collected, and trustworthiness-integrity, the user's belief that the vendor will abide by acceptable principles in information exchange, are important influences of the software users' overall trust of a vendor. The results are intended to provide guidance to software developers and government regulatory agencies in resolving the controversy surrounding spyware.

2 LITERATURE REVIEW

In this section, previous information systems research on spyware is reviewed. This research addresses user characteristics and perceptions associated with spyware, characteristics of spyware, and ethical, legal, and policy standards.

In examining consumers' awareness of spyware, Zhang (2005) found that knowledge about security, privacy, and spyware are lacking. Further, privacy invasions are not adequately noticed, nor are respondents knowledgeable in the use of spyware removal tools. Poston et al. (2005) reported that

users are generally aware of the security threat, but are not motivated to respond or to pay for anti-spyware protection. Schmidt and Arnett (2005) revealed 94% of users know about spyware, while only 61% had discovered an instance of spyware infection.

Freeman and Urbaczewski (2005) identified reasons why spyware is regarded as harmful. Privacy and performance are important issues, but privacy has greater importance. Further, users expect industry and government to regulate spyware. Awad and Fitzgerald (2005) explored what users find most offensive. Four deceptive behaviors were significantly associated with offensiveness, including changes in PC settings, slowing/crashing, installation without user consent/drive-by download, and spyware bundled with legitimate downloads. Hu and Dinev (2005) found four key determinants of whether a user takes action against spyware: awareness of spyware, perceived usefulness, perceived controllability, and perceived ease of use. Lee and Kozar 2005 reported two attitude factors, relative advantage and moral compatibility; two social influence factors, visibility and image; and two behavioral control factors, computing capacity and trialability, are significant in internet users' adoption of an anti-spyware system.

Shukla and Nah (2005) showed most spyware disseminated is adware from recreation and entertainment websites. Arnett and Schmidt (2005) purposely infected two new PCs with spyware, resulting in over 100 spyware infections from only a few websites visited, with multiple infections resulting from a single website.

Klang (2004) argued that market based protections have economic implications and foresees no legal solution, other than international consensus. Sipior et al. (2005) examined ethical and legal concerns and concluded a balance must be found between legitimate interests of spyware installers, who have obtained user consent, and users who are unwitting targets. Stafford and Urbaczewski (2004) discussed legitimate employee monitoring and non-legitimate criminal tools. There is little agreement about which programs should be regulated. Warkentin et al. (2005) addressed management and policy by proposing a 2x2 framework of consent of user to install spyware and functional consequences.

3 RESEARCH MODEL AND HYPOTHESES

The review of previous spyware research underscores the controversy surrounding spyware resulting from privacy invasion and deceptive behaviors of spyware. Consequently, we focus on internet users concerns about privacy, trust, and protection. While protection may come in the form of user vigilance, organizational initiatives, and governmental oversight, legislation, and litigation (Sipior et al. 2005), we focus on protections afforded by the United States (U.S.) legal system.

3.1 Research Model

We propose the research model presented in Figure 1 based on previous spyware research. Five variables and the relationship between them are identified, including the presence or absence of spyware in a software application, the user's belief that the software vendor is trustworthy, the user's perception of being able to control information privacy, the user's perceptions of the protection afforded by existing spyware laws, and overall trust in the software vendor. Consistent with previous research addressing trustworthiness, the user's perception of the vendor is examined as a set of specific beliefs including the ability to appropriately use any information collected, the benevolence of intentions in using information collected, and integrity in information collection and use. The presence or absence of spyware in the use of application software is hypothesized to negatively influence trustworthiness of a software package, the user's perceived control over privacy, and the user's belief that the U.S. legal system protects software users. In turn, these three variables are expected to affect the user's overall trust in the software vendor. These variables are discussed below as they relate to the use of application software within which spyware is embedded.

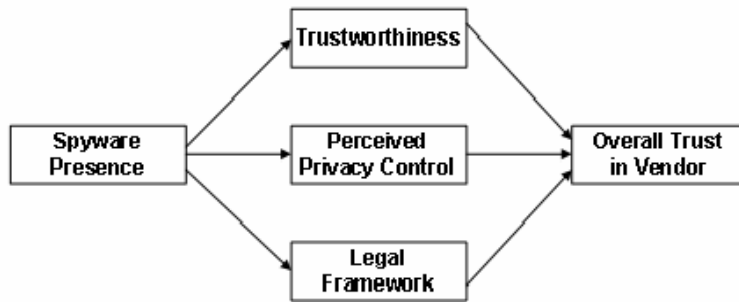


Figure 1. Research Model.

3.2 Spyware Presence

The potential for stealth spyware activity may impart an uneasy feeling during software use. Concern may be further elevated by the possibility of unwanted results such as data sharing, direct marketing, security breaches, and degraded PC performance. We therefore expect that the presence of spyware will affect users' perceptions about the use of application software within which spyware is present:

Hypothesis 1: Perceptions of trust, privacy, and legal protection will be lower for users of software with spyware than for users of software without spyware

3.3 Trustworthiness and Trust in Vendor

Trust is regarded as an emerging central aspect in the acceptance of technology (Gefen 2002). While previous research on spyware has recognized the importance of trust (Awad and Fitzgerald 2005; Hu and Dinev 2005; Klang 2004; Lee and Kozar 2005; Shukla and Nah 2005), trust was not empirically evaluated.

Trust has been conceptualized as Trustworthiness and Overall Trust. Trustworthiness is a set of specific beliefs including Integrity, Benevolence, and Ability of another entity (Doney and Cannon 1997; Ganesan 1994; Gefen and Silver 1999; Jarvenpaa and Tractinsky 1999). The general belief that another entity can be trusted (Gefen 2000) is referred to as Overall Trust. The set of specific beliefs are considered to be antecedents to the general belief (Jarvenpaa and Tractinsky 1999; Mayer and Davis 1999; Mayer et al. 1995). Based on previous empirical research on the role of trust in the acceptance of commercial websites (Gefen 2002; Jarvenpaa and Tractinsky 1999; Reichheld and Scheffer 2000), we expect a user's view of the trustworthiness of a software package to affect their overall trust of the software vendor:

Hypothesis 2: The following set of trustworthiness beliefs will be positively associated with Overall Trust

- a: Integrity will be positively associated with Overall Trust
- b: Benevolence will be positively associated with Overall Trust
- c: Ability will be positively associated with Overall Trust

3.4 Privacy Control

Without knowingly providing permission for spyware installation, the user is likely to see spyware as a violation of privacy (Sipior et al. 2005). Research on spyware has addressed users' concerns about privacy (Freeman and Urbaczewski 2005; Hu and Dinev 2005; Klang 2004; Lee and Kozar 2005; Poston et al. 2005; Shukla and Nah 2005; Sipior et al. 2005; Stafford and Urbaczewski 2004;

Warkentin et al. 2005; and Zhang 2005). Users' knowledge of internet privacy violations was empirically found to be the lowest among knowledge on security issues (Zhang 2005). We address online interaction, with a focus on user concerns with a software vendor's spyware activities resulting from actual use of that vendor's application software.

Based on Cheung and Lee (2000), we include Perceived Privacy Control to address software vendor control over privacy protection. Perceived Privacy Control refers to the users' perception of the software vendor protecting, from unauthorized use or disclosure, users' personal information collected during software use. We hypothesize that users with a high degree of Perceived Privacy Control are likely to be high on Overall Trust of the software vendor:

Hypothesis 3: Perceived Privacy Control will be positively associated with Overall Trust

3.5 Legal Framework

Previous spyware research has concluded that at its worst, spyware is a computer crime with uncertain legal consequences (Hu and Dinev 2005). The U.S. government is investigating the legitimacy of spyware (Sipior et al. 2005). However, "regulations are rudimentary" (Stafford and Urbaczewski 2005). Nonetheless, users expect industry and government to regulate problematic spyware (Freeman and Urbaczewski 2005). To assess user perceptions of legal protection, the Legal Framework variable, based on Cheung and Lee (2000), is included in this study. We hypothesize that users who believe the U.S. legal system protects software users will trust the software vendor:

Hypothesis 4: Legal Framework attitudes will be positively associated with Overall Trust

4 RESEARCH METHOD

This is an exploratory study to examine whether the presence of spyware in application software impacts users' perceptions and beliefs about trustworthiness of the application software, privacy control of the software vendor, U.S. legal protection, and overall trust of the software vendor. An experiment was undertaken using undergraduate students, who are provided with laptops as part of their degree program, as subjects. An experiment is appropriate because a field study would not allow control for the presence of spyware. The use of students as subjects may raise the question of external validity (Gordon et al. 1986). However, students are members of the online population and have an average of about 10 years of experience in this realm. Additionally, students had self-interest in taking the experiment seriously because the spyware activities would impact both them as users and their laptops. We acknowledge the limitation of the use of a convenience sample collected for this study from a specific geographic location (i.e., the mid-Atlantic U.S.).

4.1 Measures

Questionnaire items, based on previous research, were used to measure the research variables. All measurement scales were validated using factor analysis and Cronbach's alpha. The questionnaire also captured demographic information including age, college year, gender, web experience, and web use. All variables were measured using multiple items, with the exception of demographics.

4.2 Procedure

A total of 72 students enrolled in two sections of a required introductory Management Information Systems course, who had not received any formal instruction on spyware, automated data collection, or electronic commerce, served as subjects. Subjects were required to use PowerOLAP™ (Paris Technologies, Inc.), an online analytical processing software product, to retrieve data from a relational database, accessed from their laptops via an internet interface. PowerOLAP™ software was used

because it represents an unfamiliar software application and vendor. After using this software, students enrolled in the second section of the course were informed that spyware, surreptitiously collecting data during user interaction both locally and online, is embedded in PowerOLAP™ by the software vendor. A questionnaire, administered as a course requirement during class time, resulted in 35 usable responses. Subjects were appropriately debriefed, including being informed that spyware is not in fact embedded in PowerOLAP™. Students enrolled in an earlier section of the same course served as the control group. The same questionnaire was administered after PowerOLAP was used, resulting in 37 usable responses for the control group.

4.3 Subjects

Of the 72 subjects, 35 were told of the presence of spyware and 37 were in the control group. The composition of the two groups did not differ on the basis of age, sex, or computer experience. Freshmen represent 82.8% and 83.8% of the experimental and control groups, respectively. Males represent 54.3% and 56.8% of the experimental and control groups, respectively. Years of web use averaged about 10 years, with usage frequency averaging over five days per week, indicating a user population with computer experience.

5 ANALYSIS AND RESULTS

An independent samples t-test reveals partial support for Hypothesis 1. Statistically significant differences between the experimental and control group are found for Trustworthiness, Ability, Benevolence, and Overall Trust. Specifically, trustworthiness of the software vendor was significantly lower ($t = 2.25$; $p < .05$) for users of application software with spyware ($\mu = 4.60$) than for users of software without spyware embedded ($\mu = 5.21$). Among the three dimensions of vendor Trustworthiness, perceptions of vendor Ability ($t = 2.23$; $p < .05$) and Benevolence ($t = 2.82$; $p < .05$) were significantly lower for users of software without spyware ($\mu = 4.64$ for Ability; $\mu = 4.5720$ for Benevolence) than without spyware ($\mu = 5.37$ for Ability; $\mu = 5.41$ for Benevolence). Additionally, Overall Trust of the vendor was perceived to be significantly lower ($t = 2.17$; $p < .05$) among users of application software with spyware embedded ($\mu = 4.26$) versus without spyware ($\mu = 5.02$).

Multiple regression was used to test Hypotheses 2a-c, 3, and 4. An advantage of multiple regression is that an extremely large sample size of 100-200 respondents is not necessary; rather, a minimum sample size of 30 respondents is required (Gefen et al., 2000). The results of a linear regression with Overall Trust as the dependent variable and Trustworthiness, Perceived Privacy Control, and Legal Framework as the independent variables ($F = 51.142$; $p < .001$) provide support for Hypothesis 2. Trustworthiness ($t = 12.049$; $p < .000$) is a significant predictor of Overall Trust. Partial support is provided for Hypotheses 2a-c based on a linear regression with Overall Trust as the dependent variable and Ability, Benevolence, Integrity, Perceived Privacy Control, and Legal Framework as the independent variables ($F = 35.476$; $p < .001$). Specifically, Hypotheses 2a and c are supported. Ability ($t = 2.620$; $p < .05$) and Integrity ($t = 3.2677$; $p < .000$) are significant predictors of Overall Trust. Hypotheses 3 and 4 are not supported.

Limitations

Limitations of this study may be opportunities for future research. First, the use of a convenience sample collected for this study from a specific geographic location (i.e., the mid-Atlantic U.S.) limits generalizability of the results. Future research should expand the demographic representation of the online population and the geographical reach. Second, we acknowledge that directives of an instructor in a classroom environment may affect trust perceptions of the software vendor, since the students may believe that the instructor would not request student use of software which would cause privacy concerns and degraded PC functionality. Subjects, other than students in an experimental setting should be sought. Third, we acknowledge that measurement of constructs having only two items per construct may raise issues of measurement reliability, although two items is not without precedent

(Goles and Chin, 2005). Additionally, the scale for Overall Trust contains the keyword, "trust;" while not uncommon, this may introduce possible bias (Gefen, 2002). Fourth, the results are specific to one software application. Examining other types of software could increase generalizability of the results.

DISCUSSION AND IMPLICATIONS FOR RESEARCH AND PRACTICE

The capture of personal information via spyware may improve product and service offerings tailored to individual user preferences, enabling a company to develop a more intimate relationship with customers, which in turn increases trust and thereby loyalty (Reichheld and Scheffer, 2000). An enduring competitive advantage can be achieved from this cyclical interchange. Trust however, must be understood because outrage over the collection of personal data can threaten trust, resulting in a loss of loyalty. Software vendors should rethink the practice of embedding legitimate spyware in software applications, unless user trust can be maintained. To maintain user trust, software vendors must strive to balance the legitimate use of spyware with user privacy concerns. Governmental regulatory agencies may provide a clearer definition of what constitutes the legitimate use of spyware to dissuade software users' concerns.

User trust in software utilization is critical for a software vendor's success because without it, users may avoid a vendor's software should the presence of spyware be discovered. This is consistent with previous findings that consumers who lack trust in an online vendor tend not to engage in e-commerce with that vendor (Reichheld and Scheffer, 2000) and the findings that consumer trust affects both window-shopping and purchase intentions of online consumers (Gefen, 2000). However, caution is necessary since this extrapolation from online purchase intentions to actual software use has not been empirically tested.

Not only is trust vital to software vendors, it is central in the acceptance of technology. This exploratory study advances an understanding of trust by addressing actual users' perceptions of both trustworthiness and overall trust of a software vendor. Further, trustworthiness is examined as a multi-dimensional construct. The results provide support for the advantage of treating trustworthiness as a construct comprised of distinct beliefs (Gefen, 2002), allowing additional insight, for software vendors and governmental agencies, into user beliefs about trust. A vendor's trustworthiness-ability; that is, competence and knowledge about the appropriate use of private user information collected, and trustworthiness-integrity, the belief that a vendor will abide by acceptable principles in information exchange; were found to be important influences of overall trust of a vendor. A comparison of the perceptions of actual users of software with spyware, versus without, revealed lower perceptions of trustworthiness and overall trust. Specifically, a vendor's trustworthiness-ability, was perceived to be lower for actual users of software with spyware than for users of software without spyware. Vendor trustworthiness-benevolence, the extent to which the user believes a vendor's intentions in the use of information are good, was lower for users of software with spyware than without. Finally, overall trust of the vendor was lower among users of application software with spyware versus without spyware. These results offer insight into trust perceptions of software users, providing guidance for software vendors in their trust-building efforts.

CONCLUSION AND DIRECTIONS FOR FUTURE RESEARCH

Additional insights about the inclusion of spyware are needed by software vendors and government regulatory agencies. Software vendors may be concerned that users of application software within which spyware is embedded view the risks associated with spyware to be so high that they discontinue use of the software. Government regulatory agencies require insight into user perceptions and practices to determine what oversight of spyware is appropriate. The experiment undertaken was exploratory. An extension of this study would be to examine whether users actually would change their behavior by avoiding the use of software with spyware. Additionally, characteristics of the software and user satisfaction with software use may be associated with reduced user concerns. Future research could draw upon the end-user computing literature (DeLone and McLean 1992; Doll and Torkzadeh 1988; Doll et al. 1994) to explore for example, user satisfaction with the use of software with embedded spyware. Additional research will enable an understanding of the views of users

regarding the acceptability of software applications with embedded spyware, which will ultimately lead to protections for users or responses by spyware providers.

References

- Arnett, K.P. and Schmidt, M.B. 2005. "Busting the Ghost in the Machine" *Communications of the ACM*, 48(8): 92-95.
- Awad, N.F. and Fitzgerald, K. 2005. "The Deceptive Behaviors that Offend Us Most about Spyware" *Communications of the ACM*, 48(8): 55-60.
- Cheung, C. and Lee, M.K.O. 2000. "Trust in Internet Shopping: Instrument Development and Validation through Classical and Modern Approaches," *Journal of Global Information Management*, 9(3): 23-35.
- Davis, F.D. 1989. "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Quarterly*, 13(3): 319-340.
- DeLone, W. and McLean, E. 1992. "Information Systems Success: The quest for the Dependent Variable." *Information Systems Research*. 3 (1): 60-95.
- Doll, W. and Torkzadeh, G. 1988. "The Measure of End-User Computing Satisfaction." *MIS Quarterly*. 12 (2): 259-274.
- Doll, W., Xia, W., and Torkzadeh, G. 1994. "A Confirmatory Factor Analysis of the End-User Computing Satisfaction Instrument." *MIS Quarterly*, 453-461.
- Doney, P.M. and Cannon, J.P. 1997. "An Examination of the Nature of Trust in Buyer-Seller Relationships," *Journal of Marketing*, 61: 35-51.
- Freeman, L.A. and Urbaczewski, A. 2005. "Why Do People Hate Spyware?" *Communications of the ACM*, 48(8): 50-53.
- Ganeson, S. 1994. "Determinants of Long-Term Orientation in Buyer-Seller Relationships," *Journal of Marketing*, 58(2): 1-19.
- Gefen, D. 2000. "E-Commerce: The Role of Familiarity and Trust," *Omega: The International Journal of Management Science*, 28(6): 725-737.
- Gefen, D. 2002. "Reflections on the Dimensions of Trust and Trustworthiness among Online Consumers," *Data Base*, 33(3): 38-53.
- Gefen, D. and Silver, M. 1999. "Lessons Learned from the Successful Adoption of an ERP System," *Proceedings of the Proceedings of the 5th International Conference of the Decision Sciences Institute*, Athens, Greece, 1054-1057.
- Goles, T., Chin, W.W. 2005. "Information Systems Outsourcing Relationship Factors: Detailed Conceptualization and Initial Evidence." *Data Base*. 36 (4), 47-67.
- Gordon, M.E. and L.A. Slade, L.A., Schmitt, N. 1986. "The 'Science of Sophomore' Revisited: From Conjecture to Empiricism." *Academy of Management Review*, 11(1): 191-207.
- Hu, Q. and T. Dinev, 2005. "Is Spyware an Internet Nuisance or Public Menace?" *Communications of the ACM*, 48(8): 61-66.
- Jarvenpaa, S.L. and Tractinsky, N. 1999. "Consumer Trust in an Internet Store: A Cross-Cultural Validation," *Journal of Computer Mediated Communication*, 5(2): 1-35.
- Klang, M. 2004. "Spyware - The Ethics of Covert Software," *Ethics and Information Technology*, 6(3): 193-202.
- Lee, Y. and Kozar, K.A. 2005. "Investigating Factors Affecting the Adoption of Anti-Spyware Systems," *Communications of the ACM*, 48(8): 72-77.
- Mayer, R.C. and Davis, J.H. 1999. "The Effect of the Performance Appraisal System on Trust in Management: A Field Quasi-Experiment," *Journal of Applied Psychology*, 84(1): 123-136.
- Mayer, R.C., Davis, J.H., and Schoorman, F.D. 1995. "An Integration Model of Organizational Trust," *Academy of Management Review*, 20(3): 709-734.
- Paris Technologies, Inc., www.paristech.com, visited March 12, 2006.
- Poston, R., Stafford, T.F., Hennington, A. 2005. "Spyware: A View from the (Online) Street" *Communications of the ACM*, 48(8): 96-99.

- Reichheld, F.F. and Schefter, P. 2000. "E-Loyalty: Your Secret Weapon on the Web," *Harvard Business Review*, 78(4): 105-113.
- Schmidt, M.B. and Arnett, K.P. 2005. "Spyware: A Little Knowledge is a Wonderful Thing" *Communications of the ACM*, 48(8): 67-70.
- Shukla, S. and Nah, F.F. 2005. "Web Browsing and Spyware Intrusion," *Communications of the ACM*, 48(8): 85.
- Sipior, J.C., Ward, B.T., and Roselli, G.R. 2005. "The Ethical and Legal Concerns of Spyware," *Information Systems Management*, 22(2): 39-49.
- Stafford, T.F. and Urbaczewski, A. 2004. "Spyware: The Ghost in the Machine," *Communications of the AIS*, 14: 291-306.
- Warkentin, M., Luo, X., and Templeton, G.F. 2005. "A Framework for Spyware Assessment" *Communications of the ACM*, 48(8): 79-84.
- Zhang, X. 2005. "What Do Consumers Really Know about Spyware?" *Communications of the ACM*, 48(8): 44-48.