# Perceived Utility as a Motivational Factor in Affecting Users' Decisions to Download and Install Potentially Spyware-Infected Software

*Full Paper*

**Kenneth Howah**
Central Queensland University Australia
k.howah@cqu.edu.au

**Ritesh Chugh**
Central Queensland University Australia
r.chugh@cqu.edu.au

## Abstract

Spyware is acknowledged to be a growing problem in computing in the potential for privacy breaches, the theft of valuable data and facilitating the commission of other cybercrimes. This research paper is aimed at exploring perceived utility as a motivational factor in influencing user decisions to download and install free software containing spyware from the Internet. Data was collected through an online questionnaire sent to alumni of an Australian university, which was analyzed using quantitative methods. The findings revealed utility or immediate need is a strong and dominant motivating factor to download and install free software for most users even though it may be infected with spyware. The findings may have important implications for spyware proliferation and consumer protection, given the rapidly increasing uptake of online Internet activity by the general public supported by constantly improving technologies and online services.

**Keywords**

Spyware, malware, software, infected, utility, download, install, motivation, user, decision, Australia

## Introduction

Spyware is a phenomenon of, and enabled by, modern mass internetworked computing (Zhang 2005). It is not a problem of technology, but of the abuse of technology by perpetrators who gain from exploiting their victims through the use of spyware (Awad and Fitzgerald 2005; Gibson 2005a, 2005b; Sipior, Ward and Roselli 2005). Ultimately, spyware is a social problem and this means that the collective research agenda into spyware must include user-based issues (Stafford & Urbaczewski 2004). This study is aimed at contributing to that agenda.

The proliferation of spyware in a computer user's system often begins with the act of downloading free software from the Internet (Awad and Fitzgerald 2005; Federal Trade Commission 2005; Zhang 2005). When software has been *downloaded*, it is stored in the computer, but it is still not usable, active (or 'executable') by the computer. To make software active and usable by the computer's CPU, it must then be *installed*, which is the action that makes the software executable. It is following this installation stage that the spyware component is first introduced into the computer from the downloaded host software. Since downloading and installation are often two separate actions on the part of the user, questions about downloading could not be asked without asking the same questions of installation, and to determine if any relationship existed between the decisions leading to both acts.

Spyware has become prevalent in home and business computers and presents a serious threat to privacy and security (Menell 2005; Kwak, Kizzier and Euisung 2011). Users themselves are the main agent for putting spyware into computers (Good et al. 2005; Zhang 2005; Sunner 2006). Sunner expressed it as '...on balance, the weakest link in the chain will always be the user' (Sunner 2006, p.10). Understanding whether perceived utility or usefulness is actually a motivational factor that affects users' decisions to install software with spyware may contribute to more effective responses to this growing threat. If users do not perceive an application or tool to improve performance, even if it objectively does improve performance, there are very less chances of it being actually used (Alavi and Henderson 1981).

Hence, the aim of this paper is to explore perceived utility as a motivational factor in influencing user decisions to download and install free software containing spyware. Implicit in the research problem is the matter of awareness of the potential presence of spyware. The phrase 'containing spyware' implies that the user was aware of or was made aware of this potential before downloading or before installing software. The software considered as part of this study is limited to software that can be downloaded free of charge from the Internet, for private use. Commercial software, whether off-the-shelf or available for purchase online has been known to contain spyware (Stafford and Urbaczewski 2004). As commercial software is distinctly different in terms of user needs and intentions from free software that are known generally to be at risk of containing spyware, it was decided to exclude commercial software from the present study for the sake of clarity and simplicity. This study also excludes specific consideration of software downloads and installations into mobile devices such as smartphones.

Although there is extant literature available about the technology of spyware and the potential impact of spyware on individuals and businesses, there is much less research about what motivates users at the point where they are downloading or installing software, whether or not they have at least some awareness of the potential for spyware to be present. This is the point at which users would be expected to make judgmental decisions about the wisdom of proceeding first with downloading and then further with installation. Most importantly there are virtually no studies that explore whether utility was a dominant motivation for downloading free software.

This study seeks to improve understanding of perceived utility as a motivational factor in affecting users' decisions to download and install potentially spyware-infected software. The remainder of the paper is organised as follows. The next section provides a review of literature in the spyware arena. The paper then provides a brief description of the research methodology adopted for this study. Findings and discussion then follow in the successive section. Finally, the key premises of the paper have been summarised and the paper's limitations are explicitly stated with an outlook for possible future research.

## Literature Review

Spyware is part of malware, and has been characterised as 'privacy-invasive' software (Boldt et al. 2008), as 'negative technology' (Dinev and Hart 2004) and classed as a 'passive data collection technology' (Marshall and Swartwout 2006).

One of the most cited definitions is 'Spyware is any software which employs a user's Internet connection in the background (the so-called "backchannel") without their knowledge or explicit permission' (Gibson 2005b). There are many variations on this definition, but common elements are secrecy of operation; surreptitious communication with a third party; gathering of information without owner consent (Stafford and Urbaczewski 2004); and modifying network traffic along with degradation of user experience (Lavesson et.al 2011). The type of information gathered by spyware includes user actions, passwords, online purchases and other information (Sunner 2006). Much of this information gathering is not illegal, allowing the misuse of data-gathering technologies to be affectively camouflaged (Conklin 2006).

A key feature of spyware is its surreptitious nature. Users being generally aware that spyware does or may exist in the software they are downloading or installing do little to change this, since it is the ongoing existence and secretive operation of spyware that is surreptitious. Therefore, even users who may be initially aware that spyware could exist in the software they are installing tend to be thereafter unmindful of the continuous operations of the spyware in the background.

Views vary about what types of software are included under the umbrella term 'spyware'. The term 'spyware' includes adware, key loggers, trojans, hijackers, dialers and malware (Stafford and Urbaczewski 2004; Garrie, Griver, and Joller 2010). In contrast, it is not uncommon to find discussions treating adware and spyware as separate terms (Chien 2005). The main features that distinguish spyware are well known, and the numerous terms that apply to various types of spyware are usually based on the particular spyware function. Table 1 provides a summary of some terms frequently used in the literature to describe different types of spyware, or malware with spyware functions.

| **Name** | **Summary description and function** |
|---|---|
| Adware | Displays advertisements on users' desktops or windows (Stafford and Urbaczewski 2004) |
| Spyware cookies | Cookies designed to collect and steal data from computers (Dick 2007) |
| Browser/Page Hijackers | Redirects browser to alternative webpages not selected by user (Federal Trade Commission 2005) |
| Dialers | Disconnects user from their ISP and re-dials an alternative number (Spyware Guide 2006) |
| Drive-by download/Installer | Installs spyware code secretly during user visit to infected website, and avoids alerting user by exploiting browser vulnerabilities (Federal Trade Commission 2005) |
| Key loggers | Records, stores and forwards a history of users keystrokes – can be hardware device or software (Nelson & Simek 2008) |
| Trojan Horses | Disguised as, or within, genuine software; destructive in intent and opens back doors to computers to allow data theft (Swain 2009) |
| Rootkits | Conceals various spyware functions from user view by exploiting normal operating system features (Kassner 2008) |

**Table 1: Malware Categories with Spyware Functions**

While these terms refer to software with quite specific functions, other terms such as 'malware' are more generic and refer to any malicious software including viruses and worms, and these are usually treated as a separate category to spyware (Australian Government 2006). The review of literature showed that most authors concur with this view. In short, viruses and worms are about causing destruction, damage or inconvenience to their victims, while spyware is about surreptitious information mining, data theft and exploitation of stolen data. This is the general distinction, in conjunction with the definition previously outlined, that will be employed in this paper.

Conventional spyware works by residing as background processes from which they perform their designed functions. A variety of specific functions exist, but in general, all engage in user or system monitoring, data gathering, and secret communications with a third party over the victim's Internet connection. Spyware conventionally enters computer systems through downloads and installations of software that contains embedded spyware (Awad and Fitzgerald 2005; Federal Trade Commission 2005; Zhang 2005). Users are enticed into clicking on such links by the presence of bait elements, for example, a pop-up ad that says 'Urgent! You have 2 new messages' with an OK button to press. Clicking on the button redirects the user to sites capable of downloading spyware (Chien 2005).

Of concern is the trend towards malicious software including spyware being generated by professional criminals targeting victims specifically for financial gain, in contrast to the earlier dominance of amateur hackers doing it for personal reasons such as gaining malicious satisfaction or prestige within a group (Perry 2007; Williamson 2007). Thus spyware can be viewed as an evolutionary advance on viruses where to cause harm or inconvenience was the main motivator.

The prevalence of spyware has led to a numbness, or apathy, to the threat among consumers, making this a possible influencing factor in people going ahead with downloading and installing free software while at the same time being unwilling to take and pay for protective steps (Stafford 2005). The apparent blasé attitude toward this known hazard has been noted by Zhang (2005). Zhang's study of 500 Business majors' students to explore consumer general knowledge on spyware and related issues revealed that majority of respondents did not fully understand the nature of spyware and less than half took any protective action.

An experimental study by Good et al. (2005) sought to examine the factors that contribute to users' decisions to install applications that contain spyware, but with a particular focus on the effect that notices had on the decision. In general, users ignored the content of notices, and finally, on learning of the presence of spyware in some of the installed software, participants expressed some regret with their decision (Good et al. 2005).

The desired or expected functionality of software being a major factor in user decisions to download software was supported by research by Conklin (2006) who examined the factors that influence user intention to take up a technology in the context of the Diffusion of Innovations theory. One of the strongest factors identified in Conklin's study was suitability of an innovation to solve a problem, confirming this as a central factor influencing user decisions in the Diffusions of Innovation model. Several theoretical models were referenced to frame this study, but two with particular applicability were the Technology Acceptance Model and the Diffusion of Innovations Model.

Interestingly, Sriramachandramurthy, Balasubramanian and Hodis (2009) have pointed out that increased self-efficacy (belief in own ability to act or solve problems) leads to increased likelihood that defensive technologies (anti-spyware programs) will be installed and used, the corollary is often overlooked, that is, that the same self-efficacy can equally lead to an increased likelihood of users confidently downloading free software that offers solutions to other problems, thus increasing the risk of spyware infection.

Hence, it becomes apparent that some spyware exists in most computers because users have made conscious decisions to download and install software that contained spyware. At the same time, many have IT experience or knowledge, which increases their confidence, which increases self-efficacy (belief in own ability to act or solve problems). In turn, this may reasonably be construed to increase trust, and this leads to increased and extended use of online software resources, which increases the risk of contracting spyware (Saroiu, Gribble and Levy 2004).

Although a variety of literature is relevant to the topic of spyware proliferation, and generic theories are capable of providing suitable explanatory models of behaviour, much of the most relevant literature found was not written to directly address the spyware issue in context of utility. There is a paucity of scholarly research that explores whether utility motivates user decisions in respect of downloading and installing free software, with a noticeable tapering off of any studies since approximately 2006. Therefore, this study provides an up-to-date analysis that goes at least partway in filling this gap.

## Methodology

This study is concerned with human behaviour around technology. To measure relevant aspects of behaviour (perceived utility), a quantitative approach was adopted in order to discover statistically valid relationships between the likelihood of proceeding to download and installation of software containing spyware.

Data was randomly collected from a population of an Australian university's alumni using a purpose built online survey with questions tailored specifically to the requirements of the proposed study. The survey had a total of 31 questions (demographic questions, exploratory questions and direct measures of the dependent variable). However, for the purpose of this paper, we have only focussed on questions pertaining to the main triggers in deciding to install free software. Close ended questions in the questionnaire were structured using the Likert-scale format using a 5-point rating scale. The response categories for the rating scale for the close-ended questions were ordered as strongly agree, agree, neutral, disagree and strongly disagree. The questionnaire was validated by pre-testing against two separate smaller groups – one of a group of students, the other of staff, to establish basic validity, that is, the questions measure the variable that was intended. A basic test of internal consistency, the split-half method, was also performed to establish reliability using the Cronbach alpha coefficient and this returned a satisfactory result.

The use of an online survey method met more of the criteria for effectiveness than other methods (Frazer and Lawley 2000), as well as being a relatively low cost and easy to administer method (Malhotra et al. 2004). The non-discriminatory sample selection from that population base assured randomness since a large spread of demographic profiles would likely be represented despite all having the common attribute of being tertiary educated.

Email invitations for voluntarily completing the online survey were sent to 10,029 alumni, for a total response of 281 or 2.8% within an approximately three-week period. Data for this study was analysed quantitatively, consistent with the post-positivist paradigm that underpins the approach to acquiring knowledge. The data was cleaned and transformed, and then imported directly into the SPSS program for analysis.

## Findings and Discussion

The population sample consisted of 57% male and 43% female. The largest age groups were those in the ranges 31 – 40 (25.7%), followed by 41 – 50 (24.3%) and then 21 – 30 (23.2%). The majority of respondents graduated with a Bachelor's degree (57.7%). More than a third (35.6%) indicated that they had some degree of professional I.T. experience. The data indicated that most people are generally aware of the existence or potential existence of spyware in the free software they may download. Only 3.6% claim that they are not so aware. Nearly 85% claim to be "very aware" or "generally" aware.

In gathering data for this study, anecdotal evidence by email was received from a computer repair professional, on experiences with repairing malware damage on client computers. The comments corroborated findings about experience leading to carelessness. People who experience successful use of computers over time can be led to think they know more than they do. This is the reason they are not as concerned about privacy as less experienced users, since they feel that they know their computing environment. From the perspective of a computer repair professional, in reality they probably did not (Beach 2010).

It was evident from the data that downloading software, while technically a separate action from installation, does not generally lead to a different decision to installation, resulting in installation almost always following download. This meant that most factors influencing the decision to download would be nearly identical to the factors influencing the decision to install.

The factors affecting the adoption of anti-spyware are interesting, the strongest being relative advantage, that is "useful, effective in keeping computing environment safe…" (Lee and Kozar 2005). The following frequency analysis points to utility being a dominant motivator, even over-riding perceived threats and risks.

85.6% strongly agree or agree that to solve a problem is a dominant motivation for downloading free software from the Internet.

47.2% strongly agree or agree that the potential usefulness of software motivates them to download it. This is not as strong as the motivation to solve an immediate problem, showing that immediacy is important.

86.3% say they are very aware of the potential threat of spyware whilst downloading free software from the Internet. This is not enough to deter them from downloading such software if there is an immediate need, unlike in the case where there is no immediate need but the software appears to be potentially useful. Thus we can conclude that immediate utility is strong enough to overcome constraints based on knowledge of threats.

84.6% are at least generally aware of the potential presence of spyware in any software they might download. Noting again the similar percentage to those downloading when motivated by the need for utility, it again shows that knowledge of potential threat is overcome by the immediate benefit offered by the free software.

The data shows that immediate utility is the strongest motivator for downloading software, and is confirmed as a powerful motivator for computer users to download and use any kind of software, and affectively overcomes constraining factors, such as knowledge of potential threat. The data analysis rested on two basic assumptions about the sample with frequency analysis conducted to support these assumptions. These were:

i) That people are generally aware of the existence or potential existence of spyware in the free software that they download.

ii) That people are generally aware that spyware poses a threat to them.

Data analysis confirms these assumptions. The strongest factors influencing decisions to download free software are the potential for the software to solve a problem and to be useful, and both of these can be described as aspects of utility. Other measured factors such as the "cool" factor, interesting factor, and handy factor were not accepted as strong motivators to download, leaving the pragmatic factors of problem solving and usefulness (that is, utility) as the dominant factors.

The dominance of utility as a motivating factor in high-risk online behaviour was shown in data compiled by Pew Internet & American Life Project May-June 2005 survey cited in Fox (2005). This data showed that of 188 respondents who reported an incidence of spyware infection, 46% had engaged in risky behavior such as playing online games, sharing files or visiting adult sites. The main motivator of utility in the sense of entertainment is consistent with the finding of utility in the broader sense of 'solving a problem' in the present study, and both findings are consistent with 'utility' or usefulness as a major motivator in well-known behavioural models such as the Technology Acceptance Model (Larsen et al. 2015).

The basic argument concerning utility in this study has relied on quantitative data analysed using standard frequency analysis techniques. It is acknowledged that since we are in reality analysing facets of human behaviour, there will always be a possibility that some may find our conclusions more convincing than others.

## Conclusion

The study has demonstrated that perceived utility of free software to solve a problem is a dominant deciding factor in whether to download and install. First and foremost, software on offer on the Internet has strong utility appeal, that is, the software is seen as useful and capable of helping the user to solve a present problem. In many ways this finding is intuitive, since Internet content that is not actually useful tends not to survive. However, the finding includes the fact that utility (the promise of a solution) is a strong enough attractant to override knowledge of potential threats.

It is worth noting that in general, any voluntary survey-based study of this topic is likely to suffer from some response-bias risk. In this study some degree of response bias in participants heavily interested in IT cannot be entirely discounted, and therefore, generalizability even within the study population must be circumspect.

As this study excluded those with no experience of tertiary education, further studies could look at samples that include this group. The effect of different education levels on spyware proliferation may then be investigated and could have applicability in terms of the broader population. Internet users in general trust the Internet and whilst this study looked at utility alone, further studies could look at trust issues in downloading and installing spyware infected software.

It is clear that spyware is part of other, often legitimate, software, and is not something downloaded as a stand-alone function. In this respect, the secrecy aspect of spyware becomes highly relevant. By definition, spyware does not overtly present to potential downloaders as 'spyware', but always as code embedded in other apparently legitimate or harmless computer programs. Awareness of potential presence therefore becomes an issue. Whilst the anticipated utility of downloaded software is a dominant factor that usually overrides suspicion or caution, it is still important that Internet users make informed judgmental decisions when downloading free software that could be potentially infected with spyware.

## *References*

Alavi, M. and Henderson, J.C. 1981. "An Evolutionary Strategy for Implementing a Decision Support System," *Management Science*, (27:11), pp. 1309-1323.

Australian Government. 2006. "More Malware – Adware, Spyware, Spam and Spim," *Australian Institute of Criminology*, (11), pp. 1-2.

Awad, N.F. and Fitzgerald, K. 2005. “The Deceptive Behaviors that Offend us most about Spyware,” *Communications of the ACM* (48:8), pp. 55-60.

Beach, L. 2010. “Have a Say - Participate in the Spyware Research Survey”, 22 September 2010, Email.

Boldt, M., Jacobsson, A., Lavesson, N. and Davidson, P. 2008. “Automated Spyware Detection Using End User License Agreements”, *International Conference on Information Security and Assurance*, Busan, 24- 26 April, pp. 445-452.

Chien, E. 2005. “*Techniques of Adware and Spyware*”, pp. 1-33, viewed 15 February 2015, http://www.symantec.com/avcenter/reference/techniques.of.adware.and.spyware.pdf

Conklin, W.A. 2006. “Computer Security Behaviors of Home PC Users: A Diffusion of Innovation Approach,” *Doctor of Philosophy thesis*, University of Texas, San Antonio.

Dick, J. 2007. “What Makes a Cookie a Spyware Cookie?,” *Ezine Articles*, viewed 10 January 2015, http://ezinearticles.com/?What-Makes-a-Cookie-a-Spyware-Cookie?&id=716437

Dinev, T. and Hart, P. 2004. “Internet Privacy, Social Awareness, and Internet Technical Literacy - an Exploratory Investigation”, *17th Bled eCommerce Conference*, Bled, Slovenia, 21-23 June, pp. 1-12.

Federal Trade Commission. 2005. “Monitoring Software on Your PC: Spyware, Adware, and Other Software,” *Federal Trade Commission*, viewed 10 January 2015, http://www.ftc.gov/os/2005/03/050307spywarerpt.pdf

Fox, S. 2005. “*The Threat of Unwanted Software Programs is Changing the Way People Use the Internet*', viewed 11 January 2015, http://www.pewinternet.org/files/old-media/Files/Reports/2005/PIP_Spyware_Report_July_05.pdf.pdf

Frazer, L. and Lawley, M. 2000, *Questionnaire Design and Administration*, Milton, Qld, Australia, John Wiley & Sons Australia Ltd.

Garrie, D.B., Griver, Y., and Joller, M. 2010. “Regulating Spyware: Challenges and Solutions,” *Journal of Internet Law*, (13:8), pp. 3-13.

Gibson, S. 2005a. “Spyware was Inevitable,” *Communications of the ACM*, (48: 8), pp. 37-39.

Gibson, S. 2005b. “*Internet Connection Misuse & Abuse*”, viewed 10 January 2015, https://www.grc.com/optout.htm

Good, N., Grossklags, J., Thaw, D., Perzanowski, A., Mulligan, D. and Konstan, J. 2006, “User Choices and Regret: Understanding Users' Decision Process about Consensually Acquired Spyware,” *I/S: A Journal of Law and Policy for the Information Society*, (2:2), pp. 283-344.

Kassner, M. 2008. “*10+ things you should know about rootkits*,” viewed 10 January 2015, http://www.techrepublic.com/blog/10-things/10-plus-things-you-should-know-about-rootkits/

Kwak, D., Kizzier, D.M., and Euisung, J. 2011. “Spyware Knowledge in Anti-Spyware Program Adoption: Effects on Risk, Trust, and Intention to Use,” *44th Hawaii International Conference on System Sciences (HICSS)*, Kauai, Hawaii, 4-7 January, pp. 1-10.

Larsen, K.R., Allen, G., Vance, A. and Eargle, D. 2015. “Theories used in IS Research Wiki,” viewed 12 January 2015, http://IS.TheorizeIt.org

Lavesson, N., Boldt, M., Davidsson, P., and Jacobsson, A. 2011. “Learning to detect spyware using end user license agreements,” *Knowledge & Information Systems*, (26:2), pp. 285-307.

Lee, Y. and Kozar, K.A. 2005. “Investigating Factors Affecting the Adoption of Anti-Spyware Systems,” *Communications of the ACM*, (48:8), pp. 72-77.

Malhotra, N., Hall, J., Shaw, M. and Oppenheim, P. 2004. “*Essentials of Marketing Research: An Applied Orientation*,” Frenchs Forest, Pearson Education Australia.

Marshall, K.P. and Swartwout, N. 2006. “Marketing and Internet Professionals' Fiduciary Responsibility: A Perspective on Spyware,” *Journal of Internet Commerce*, (5:3), pp. 109-126.

Menell, P.S. 2005. “Regulating ‘Spyware’: The Limitations of State ‘Laboratories’ and the Case for Federal Preemption of State Unfair Competition Laws,” *Berkeley Technology Law Journal*, (20:3), pp. 1363-1418.

Nelson, S.D. and Simek, J.W. 2008. “Adultery in the Electronic Era: Spyware, Avatars, and Cybersex,” *Journal of Internet Law*, (11:11), p. 18.

Perry, C. 2007. “Evolving Security Threats Create Challenges,” *Processor*, (29:28), viewed 12 January 2015, https://archive.org/stream/processor-newspaper-v29i28/P___2928_djvu.txt

Saroiu, S., Gribble, S.D. and Levy, H.M. 2004. “Measurement and Analysis of Spyware in a University Environment,” *Proceedings of the ACM/USENIX Symposium on Networked Systems Design and Implementation (NSDI)*, San Francisco, CA, USA, March 2004.

Sipior, J.C., Ward, B.T. and Roselli, G.R. 2005. “The Ethical and Legal Concerns of Spyware,” *Information Systems Management*, (22:2), pp. 39-49.

SpywareGuide. 2006. "*Intro to Greynets and Spyware*," viewed 10 January 2015, http://www.spywareguide.com/txt_intro.php

Sriramachandramurthy, R., Balasubramanian, S.K. and Hodis, M.A. 2009. "Spyware and Adware: How Do Internet Users Defend Themselves?," *American Journal of Business*, 24 (2), pp. 41-52.

Stafford, T.F. (2005). "Consumer Apathy and the Emerging Revenue Model of the Internet: The Economic Case for Spyware," *Journal of Electronic Commerce in Organizations*, (3:4), pp. 1-4.

Stafford, T.F. and Urbaczewski, A. 2004. "Spyware: The Ghost in the Machine," *Communications of the Association for Information*, (14), pp. 291-306.

Sunner, M. 2006. "Spyware: Know Your Enemy," *MessageLabs*, viewed 10 January 2015, http://eval.symantec.com/mktginfo/downloads/WP3_WAA_Spyware_Know_Your_Enemy.pdf

Swain, B. 2009. "*What are malware, viruses, Spyware, and cookies, and what differentiates them*?," 10 January 2015, http://www.symantec.com/connect/articles/what-are-malware-viruses-spyware-and-cookies-and-what-differentiates-them

Williamson, M. 2007. "A Conversation with Jamie Butler," *ACM Queue*, (5:1), pp. 16-23.

Zhang, X. 2005. "What Do Consumers Really Know About Spyware?," *Communications of the ACM*, (48:8), pp. 44-48.