By Merrill Warkentin, Xin Luo, *and* Gary F. Templeton

A Framework for Spyware Assessment

The formulation of spyware policy must be a global effort and should reflect an understanding that not all spyware is bad.

One of the most challenging problems confronting the IT community is responding to the threat of spyware. Recent research, legislative actions, and policy changes have been hastened to counter spyware's threat to the privacy and productivity of both individuals and organizations [2, 10–12].

"To me, it all comes down to good manners—when I invite someone into my home, or in this case my computer, I expect them to behave and leave when asked."

—Cliff Stearns (R-FL), on his reason for drafting an amendment to the Spy Act.

As with any new phenomenon, definitional guidance must be established among the community of stakeholders (such as societal and organizational policymakers and IS managers and researchers) before adequate policies and practices can be asserted. This article fills a definitional void by articulating a framework that can guide and organize future discourse on the spyware topic, and suggests how the framework might be applied to the legislative domain.

Many prominent definitions of spyware are specific and focus on surreptitious [4] communication over the Internet [1, 3] that cause negative consequences [6] to the direct user (the individual whose machine has been infiltrated). We have two problems with these perspectives. First, we believe that the secret nature of spyware is becoming increasingly less applicable. Specifically, many spyware components use the veiled approach of placing the intention to monitor notification within End User License Agreements (EULAs) immediately before the installation of other programs. But because users commonly accept the EULAs without being aware they are installing software that will monitor their activities, there may be consent without awareness, certainly not true informed consent.

Second, spyware does not necessarily damage the direct user [9], as many definitions imply. We argue that a remote user (the provider of this software) may monitor the activity of a direct user in a mutually beneficial way. For this reason, we choose to present a more comprehensive view in an effort to provide direction for a wide variety of spyware stakeholders.

We define spyware here as a client-side software component that monitors the use of client activity and sends the collected data to a remote machine. (Later, we define spyware with greater specificity by establishing four distinct classes). This definition does not imply the software component exists without the knowledge of the *direct user* (the individual using the client); nor does it exclude direct users who benefit from such spyware components.

Spyware is resident client-side because, presumably, any evidence of direct-user activity detectable only on the server side is legitimate because the user willingly sent such evidence. In the proposed definition, software might encompass any script or executable code, any cookie data or similar client-side data that can be read by the server, or any API, applet, or software feature that can be read by the server. Such software may be either an embedded component or a standalone application. Monitored activities might include keystrokes, visiting Web sites, downloading images, or saving data.

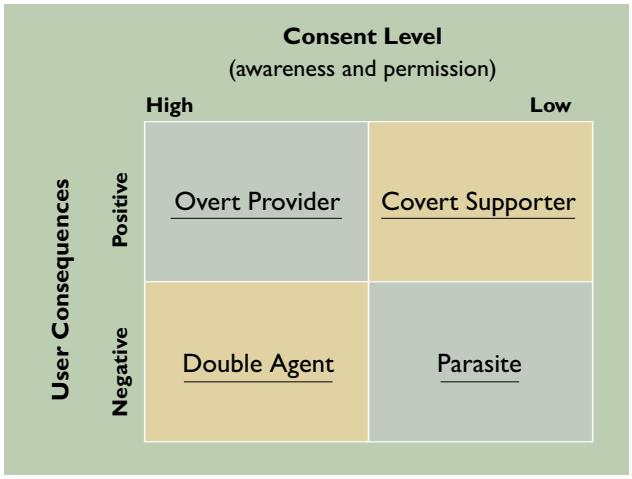
Under this definition, monitoring that occurs within the organization and is not being shared remotely does not qualify as spyware. Furthermore, client-side software must exist for a software component to be classified as spyware. For example, the software used by grocers to observe purchase habits via the loyalty card at checkout counters is not spyware. However, if the shopper visited an online grocer and client-resident software is used to observe the user clickstream, then the grocer could be said to be employing spyware.

A Proposed Framework

To support the ongoing identification and management of spyware, we propose a framework based on two key considerations: user consent and user consequences. Consent is the extent to which the user has agreed to allow a given software component to be installed and executed. Consequences are the extent to which the component provides a beneficial functionality to the direct user. Note that consent and consequences are not binary in nature—they are continua. When interacting with software, users may exhibit varying degrees of consent and simulta-

neously varying degrees of consequences. For instance, many users have a vague understanding of cookies and accept them contingent upon a variety of circumstances. The accompanying figure, constructed using these two perspectives, details four distinct characterizations of spyware.

First, the *overt provider* is the category of spyware whereby users consent to its existence and receive positive consequences. Overt providers instigate the considerable prevalence of adware that e-business companies exploit to monitor and analyze user behavior for business promotion and advertisement purposes. For example, adware is a widespread form of spyware that monitors online activities and triggers advertisements in response to selections. It commonly proliferates by being bundled in P2P and other free software.



A spyware framework.

Because of their positive consequences, users may not want to be constrained from using overt providers. In fact, many overt providers add some measure of usefulness and convenience to users. One of the more useful aspects of spyware is the use of globally unique identifiers (GUID) to collect customer information (including name, address, preferences, and contact information) that is shared within a network of interlinked Web sites to better serve the user. Subsequently, each user is then uniquely identified using the GUID. Such spyware GUID applications expedite the use of passwords and personalized information updates (such as local events, local weather conditions, and product browsing).

For example, WhenU.com is an adware company that provides customers with information on bargains and online savings by examining keywords, URLs, and search terms favored by the user. Similarly, client-side spyware can also help users solve computing problems, such as unresponsive applications. Microsoft's Error Reporting Service collects data about machine configuration and network connections and sends it to its Online Crash Analysis server to help diagnose software problems so that service patches can be developed and made available to the user community (see oca.microsoft.com/en/dcp20.asp).

Second, the *double agent* is a particularly devious form of spyware. It has the user's consent, but is damaging to the direct user. These spyware components plant damaging information (such as pornography, performance-hindering settings, or viruses) and then advertise services to the user to manage the problem or remove the offending components, but which then promulgate negative consequences, much like a Trojan. This scenario involves a confounded relationship between user and spyware provider. In this case, the user may not be aware of the spyware installation, which can also be installed a number of discrete ways (for example, bundling with other applications, providing no option to deselect during the installation of another program, or including spyware acceptance in lengthy EULA agreements).

For example, Xupiter launches pop-up ads, changes default home pages, redirects mistyped or incomplete URLs to affiliate sites and redirects search requests to off-brand search sites. Once resident, this software further promotes itself by adding Xupiter links to bookmarks and blocking attempts to restore original browser settings. Xupiter also has an imposing privacy policy, which notes that the "company" or its partners may deliver programming fixes, updates, and upgrades via automatic updates. Users are also advised that conflicts may occur with other applications and that Xupiter will determine what those applications are so that the company can resolve these conflicts whenever possible. Several versions of Xupiter download other programs such as gambling games onto affected computers [4].

Third, the *covert supporter* is hidden software that provides positive consequences. For instance, helpdesk personnel have commonly provided support to users by viewing client screens remotely via network monitoring software. Most network middleware allows administrators to monitor and observe network traffic for various productive purposes, including intrusion detection or ensuring adherence to corporate IS use policies. Covert supporters are also commonly designed to monitor user activities, such as the Web sites visited, email, and IM communications, mainly to promote online performance.

A common example of the covert supporter is browser cookies [7], which personalize interfaces

based on previous user behavior and may also generate pop-ups that greet and promote products to the user. Another example of the covert supporter is ComScore Network's Marketscore, which is a free downloadable application that increases Internet surfing speed and protects email from viruses, but also tracks user habits and compiles statistical data for industry research.

Note that some situations may dictate that improvements to system performance are undesired. In particular, the prevalence of online pornography and other risks is of particular interest to many parents. To mitigate these risks, parents can install spyware on home systems to remotely monitor and protect their interests as parents. This form of spyware would not be effective if the users (children) knew of its existence.

Finally, the *parasite* is spyware that does not have user consent and promulgates negative consequences. Many users might be surprised that they are under the ongoing remote surveillance of malevolent invaders. Drive-by downloading (as noted throughout this section) clandestinely proliferates spyware when a user visits certain URLs. Such programs can degrade performance and are designed to make removal as difficult as possible. Indeed, keystroke loggers are potentially the worst category of spyware because they can steal sensitive user or organizational information.

Most user complaints about spyware stem from parasites due to the extent of damage and difficulties associated with their recognition. The parasite is especially troublesome because the user may be exposed to incriminating information (such as pornography) and privacy can be breached without user consent. Significant negative consequences of parasites include both user and organizational concerns. The most damaging user consequence includes privacy violations, which may include the capture and recording of sensitive user information (for example, bank account numbers, contact information, and Social Security numbers). Additionally, parasites affect businesses by stealing user names and passwords to launch attacks, gain access, and impair performance. Attacks may include downgrading machine performance (in terms of high CPU usage and network bandwidth occupancy), redirecting browsers to spyware-affiliated addresses, and displaying pop-up advertisements that plague user screens.

Applying the Framework to Legislative Control

Recent legislative actions in the U.S. will serve as a platform for understanding the public policy perspective on spyware assessment. Other nations are similarly considering or enacting various laws that apply to certain categories of software defined as spyware, though there is no universally recognized definition of this software. The U.S. House of Representatives passed the Internet Spyware Prevention Act of 2004 and the Spy Act, which would prohibit taking control of a computer, surreptitiously modifying a Web browser's home page, disabling antivirus software without proper authorization, intentionally exceeding authorized access, causing injury through unauthorized installation of spyware, or secretly accessing personal data. Industry pundits are already saying this legislation will be ineffective.

Earlier versions of this legislation were opposed (by the U.S. Chamber of Commerce and others) because the broad wording would prevent legitimate software, inhibit e-commerce, and create new legal liabilities. The Spy Act specifically requires an opt-in notice and consent form for legitimate software that collects personally identifiable information from consumers. Interestingly, the legislation also permits vendors to check computers without consent and notice to determine whether the user has unauthorized installation of their software.

The U.S. Senate version of this legislation, now under consideration, is the Software Principles Yielding Better Levels of Consumer Knowledge Act, better known as the SPYBLOCK Act, which incorporates stringent disclosure requirements if software has specific features, such as those that:

- Collect user information and transmit it over the Internet to a third party;
- Cause pop-ups or other advertisements to appear on the user's machine;
- Transmit messages or data over the Internet to third parties for purposes unrelated to any task the computer user is intentionally performing using the computer, such as hijacking the user's computer to send spam or to perform other tasks; and
- Modify user settings without the user's consent, such as automatically changing the designated home page on the user's Web browser.

(Note that U.S. Senate versions and those from the U.S. House of Representative must be merged into a "compromise bill" then forwarded to the President for a signature before becoming law.)

Utah is the first state in the U.S. with spyware laws in place, and they will soon be tested in court. California, New York, Iowa, Virginia, and other states may soon follow. A similar European Com-

mission privacy directive has been in place since 2002. All these legal measures call for notice, consent, and ease of removal. However, some (such as Utah's) are more consumer-oriented, with a more stringent position on acceptable software, and others (such as California's) are oriented more toward the technology industry, which fears that legislation could outlaw certain existing practices.

The proposed framework can be used to show a strong need for a more comprehensive perspective on spyware legislation. We believe the framework can reduce confusion in the drafting of effective policy controls (that is, legislation and corporate policy). This research casts a wide net in defining and describing spyware because we believe consent and consequences have not been adequately addressed in prevailing policies, legislation, and anti-spyware applications.

Why are the distinctions between positive and negative consequences important? If legislators enact laws without clear specification, unintended outcomes could ensue. Laws and statutes may be written that could make valid corporate network monitoring illegal. Lumping all cookies that track activity or user identity together with malicious spyware creates confusion. We offer these examples indicating a greater appreciation for the full range of spyware types along the consent and consequences continua:

- Cookies were conceived by Lou Montulli, a software engineer for Netscape, to facilitate shopping cart applications and personalization, and this is still their primary use, one which brings significant benefit to millions of Internet users. (Many users are disappointed when they disable cookies and find they must search for their passwords, must log back into many media sites, and can no longer buy books or other products from their favorite Web sites.)
- Leading anti-spyware products, such as Lavasoft Ad-Aware and Spybot Search and Destroy have labeled a wide variety of valid products as spyware. These include a promising new Web-based product category called "researchware," such as ComScore Networks' Marketscore, which is installed on more than one million PCs in the U.S. Researchware is being adopted rapidly by numerous prominent companies, universities, and media outlets. ComScore Networks and other researchware providers and their customers in industry, academia, and the media are concerned that popular anti-spyware applications are targeting their applications for removal, even though they believe their applications provide positive functional benefits to both users and their clients.
- Lavasoft Ad-Aware identifies all applications as spyware if they remember what your most recent files were or where you prefer to save your work. This functionality is clearly beneficial to the user and should not be offered to unsuspecting users for removal.

WHY ARE THE DISTINCTIONS BETWEEN POSITIVE AND NEGATIVE CONSEQUENCES IMPORTANT?

If legislators enact laws without clear specification, unintended outcomes could ensue.

Other technologies offer useful perspectives on this issue, and may even be affected by proposed legislation, given that computers are now found in a wide variety of products. If legislation were drafted incorrectly, would phone companies that provide us with Caller ID services be guilty of installing spyware? What would be the impact of proposed legislation on Motor Vehicle Event Data Recorder (MVEDR) technology, commonly called automotive black

boxes, which are already installed in over 40 million cars for electronically monitoring driver activity and providing information to the insurance industry after collisions, and which are typically installed into automobiles without owner's awareness and consent?

Conclusion

Policy formulation must be based on common sense. Rep. Cliff Stearns drafted an amendment to the Spy Act that adds fines, browser hijacking, keystroke logging, and unclosable ad serving. He says "To me, it all comes down to good manners—when I invite someone into my home, or in this case my computer, I expect them to behave and leave when asked." But laws (and corporate security policies) must also be very carefully worded to protect and promote positive functionality.

The first contribution of this study regards definition. Stafford and Urbaczewski suggest in [10] an agenda for further research on spyware. The first step is adequate research by the IS community that describes the spyware problem. This article contributes by proposing a general definition of spyware dependent upon the context of use. Furthermore, we articulate a more precise framework that can be used to organize thought on the subject. We believe it is imperative that developers, software vendors, managers, scholars, users, and others establish and use frameworks to guide their work in this area. Further, the four proposed characterizations are applicable to a wide range of situations in practice.

Confusion over spyware has caused many companies to refrain from adequately implementing spyware solutions. Spyware is not understood as well as other security threats (such as P2P, viruses, worms, and hacking). Thus, one contribution of this article is a comprehensive framework for defining and classifying the thousands of spyware applications deployed globally. The use of this framework would facilitate the development of relevant solutions and strategies to address the problem.

The second contribution of the framework is a discussion that may lead to progress and the establishment of clear legal and policy standards. Stafford and Urbaczewski [10] also suggest we must track legislative and regulatory activity. Here, we review some recent legislative activity and show a need for the proposed framework. In summary, policymakers should be wary of blocking spyware applications that have positive consequences, even if those applications do not have consent.

We conclude that the most profound danger in spyware litigation is the risk of "throwing out the baby with the bathwater." Will legislation make legitimate software components difficult or impossible to distribute? Will parents who use "SpyBuddy Stealth Edition" to monitor their children's Internet activity risk prosecution? Will Web sites that create electronic communities of users be guilty if they fail to properly inform the users of the information they are sharing? We urge the global community to use this framework to organize research and policy agendas as spyware continues to become a mainstream global computing issue. C

References

1. Ames, W. Understanding spyware: Risk and sesponse. *IT Pro 6,* 5 (2004), IEEE Computer Society, 25–29.
2. Bruening, P.J. and Steffen, M. Spyware: Technologies, issues, and policy proposals. *J. Internet Law 7*, 9 (2004), 3–8.
3. Chow, S.S.M., Hui, L.C.K., Yiu, S.M., Chow, K.P. and Lu, R.W.C. A generic anti-spyware solution by access control list at kernel level. *J. Systems and Software 75,* 1–2 (2005), 227–234.
4. Delio, M. Spyware and adware rogues' gallery. *InfoWorld 40* (2004), 35–41.
5. *eWeek.* Bill sends spyware, adware purveyors down divided paths; www.eweek.com/article2/0,1759,1708763,00.asp (accessed Apr. 20, 2005).
6. Goth, G. Spyware: Menace, nuisance, or both? *IEEE Security & Privacy 1,* 3 (2003), 10–11.
7. Hormozi, A.M. Cookies and privacy. *Information Systems Security 13,* 6 (2005), 51–60.
8. Network Associates. Network Associates Introduces McAfee AntiSpyware—Essential Protection Against Spyware for Consumers (2004); www.net-security.org/press.php?id=1973 (accessed Mar. 15, 2005).
9. Sariou, S., Gribble, S.D. and Levy, H.M. Measurement and analysis of spyware in a university environment. In *Proceedings of the ACM/USENIX Symposium on Networked Systems Design and Implementation* (San Francisco, CA, 2004).
10. Stafford, T.F. and Urbaczewski, A. Spyware: The ghost in the machine. *Commun. AIS 14* (2004), 291–306.
11. Urbach, R.R. and Kibel, G.A. Adware/spyware: An update regarding pending litigation and legislation. *Intellectual Property & Tech. Law J. 16*, 7 (2004), 12–17.
12. Volkmer, C. Should adware and spyware prompt congressional action? *J. Internet Law 7*, 11 (2004), 11–18.

Merrill Warkentin (mwarkentin@acm.org) is a professor of MIS in the College of Business & Industry at Mississippi State University, Mississippi State, MS.
Xin Luo (XL96@msstate.edu) is a Ph.D. candidate in MIS at Mississippi State University, Mississippi State, MS.
Gary F. Templeton (gtempleton@cobilan.msstate.edu) is an assistant professor of MIS at Mississippi State University, Mississippi State, MS.