Communications of the Association for Information Systems

SPYWARE: THE GHOST IN THE MACHINE

Thomas F. Stafford
Management Information Systems Department
University of Memphis
tstaffor@memphis.edu

Andrew Urbaczewski
School of Management
University of Michigan – Dearborn

ABSTRACT

Computer users face a new and growing threat to security and privacy. This threat is not in the form of direct attacks by viruses or hackers, but rather by indirect infiltration in the form of monitoring programs surreptitiously installed on computers. These monitoring applications are called spyware, and serve to record and transmit a user's computer uses and behaviors to third parties. Frequently used by marketers to harvest customer data for segmentation and targeting purposes, spyware can serve to direct targeted advertising to computers. Spyware is often legally used since installations can be authorized as part of the licensed "clickwrap" agreement that users agree to when downloading free utility and file sharing programs from the Internet. In some cases, spyware is installed as part of legitimate computer applications provided by business to their customers, to provide updating and communicative functionality to application users. It appears that the ability to monitor remotely and communicate with computers is an opportunity attractive enough to attract the attention of third parties with non-legal intentions. This article focuses on the roles and functions of spyware, its use in both legitimate and non-legitimate ways, and a range of preventions and protections for avoiding and removing spyware that has been installed on end user computers.

Keywords: spyware, computer security, privacy, internet, hackers, surveillance

I. WHAT IS SPYWARE?

At last count, over 78,000 applications were designed to monitor and report computer user activities remotely [Metz, 2004]. While a range of fine distinctions can be drawn between various remote monitoring and reporting programs, most people simply refer to this class of programs as "spyware." It is estimated that spyware is now installed on over 85% of personal computers [Farrow, 2003]. A recent survey by an Internet Service Provider found an average of 28 spyware items installed per user computer. A few computers come directly from the manufacturer with spyware applications installed on them [Levine, 2004; Thompson, 2003]. Spyware, as a general class of remote monitoring applications, is a problem that has become so severe that network

administrators consider it a greater threat than unsolicited email [Berman, 2004; Townsend, 2003]. Yet, little empirical work exists to establish the prevalence and magnitude of the problem [Beales, 2004].

John Edwards, the Democratic candidate for United States Vice President in the 2004 election said: "Spyware is just one of many startling examples of how our privacy is being eroded" [Edwards, 2001]. Senator Edwards is one of several members of the U.S. Congress who attempted or are currently attempting to limit the influence and effect of spyware on the computer-using public.

Internet software developer Steve Gibson is considered to have coined the term "Spyware" for a class of software agents that reside on user computers and provide access and information to outside parties via network connections [Schwartz, Davidson and Steffan, 2003]; Gibson believes that any application that surreptitiously (that is, without user knowledge and/or permission) uses a computer's Internet "back channel" to communicate with an external server should be considered a case of spyware, since the application opens a secret communications channel from the computer to the outside world [Gibson, 2003]. Similarly, PC Magazine maintains that any application that tracks user behavior without their knowledge and consent is spyware, regardless of its specific intent or legality [Metz, 2004].

DEFINITIONS

Spyware is the name given to the class of software that is surreptitiously installed on a user's computer and monitors a user's activity and reports back to a third party on that behavior [Anon, 2004; Daniels, 2004; Doyle, 2003; Taylor, 2002]. The Federal Trade Commission, which probably carries the most potent regulatory authority to control spyware, defines it as software that aids in gathering information about a person or organization without their knowledge, and that may send that information to another entity without user consent [Urbach and Kibel, 2004]. Spyware, essentially, is software that asserts control over a user's computer without his/her consent.

"Spyware" includes:

- Adware,
- Key Loggers, and
- Trojan Horses [Internet Journal, 2002; Levine, 2004; Schwartz, Davidson and Steffan, 2003].

These applications at best consume computer resources and bandwidth and at worst lead to egregious security issues in the user computer [Townsend, 2003].

Adware

Applications that are characterized as Adware perform a range of functions:

- They monitor user Web browsing activity and send targeted advertisements to the user desktop based on that browsing activity,
- They can actually change the way a users' Web browser works by the installation of "browser helper objects," and
- They can change the default settings of Web browsers to display different home pages and bookmark lists and redirect searches to different search systems [Levine, 2004].

Many remote monitoring adware applications are characterized by their creators as legitimate business uses [Internet Journal, 2002], and are designed in accordance with specific business

models designed to direct targeted pop-up ads to users in the context of their online browsing and search activity [Naider, 2004].

Keystroke Loggers

User monitoring software existed in many forms prior to the personal computing age. Programs designed to capture logon ID and password information on mainframe dumb terminals were available in the 1970's [Ferrer and Mead, 2003]. Some key loggers are marketed as legitimate tools for tracking employees or family members [Internet Journal, 2002], but despite the putative legitimacy of some keystroke loggers, this form of spyware continues to be a highly prevalent and threatening form of the genre. Reasons for the use of "activity monitors"[1] range from genuine concern, in the case of parents or employers monitoring their charges for appropriate Internet use, to the highly illegitimate, in the case of identity theft or outright spying [Baldwin and Klingdon, 2003; Levine, 2004].

Key loggers are also used by hackers to capture passwords and infiltrate target networks, as was the case with the invasion of the Microsoft's Redmond, WA office network [Farrow, 2003]. Often they are installed as part of Trojan Horse attacks. Keystroke loggers can also take the form of mechanical devices attached to the computer keyboards [Baldwin and Klingdon, 2003].

Rats (Remote Administration Trojans)

Trojans are named after the Trojan Horse tactic of Greek history, where something unknown and unexpected comes delivered in a package that a user might normally accept; typically a free software download such as a computer game or peer-to-peer file sharing program [Internet Journal, 2002]. Trojan horse attacks, or simply "Trojans," involve installing programs that can be contacted by outside computers and which provide control over the host computer. The characteristic label for this class of spyware is "RAT" (short for Remote Administration Trojan). Their threats range from common dialer programs designed to engage user modems to incur expensive "900-number" toll charges, to more nefarious modifications of network administration tools such as Back Orifice or SubSeven, which exploit holes in the Microsoft operating system to give outside users the ability to capture screen displays and keyboard input or actually take control of a remote computer [Carfarchio, 2002; Internet Journal, 2002].

These remote administration forms of spyware are clearly malicious. Although remote administration as a general practice is one of the many techniques legitimate network administrators use to monitor and control the networks for which they are responsible, these Trojans have no particular business application or legitimating use. However, the typical RAT is a case of viral malware (e.g., [Carfarchio, 2002]), arriving as an email attachment or as a drive-by download [e.g., Mikusch, 2003]). RATs attack by exploiting weaknesses in the Microsoft browser or operating system to install itself and then trigger installation of utilities that monitor and control the target computer for malicious purposes as mild as Web site re-directs and as threatening as zombie-like production and transmission of bulk email spam [Fisher, 2004].

Criminal Tools

Although many believe that spyware applications are still relatively innocuous and benign [Shultz, 2003], expectations of technology futurists at Gartner are that spyware will soon be the tool of choice for identity theft operations, including password harvesting, and credit card number theft [Radcliff, 2004].

Illegal spyware can take many forms, including Browser Hijackers, Dialers, Drive-By Downloads, Scumware [Mikusch, 2003]. A common characteristic of each variant is that they are designed to

[1] This sort of software can record not only keystrokes, but also screen shots, mouse movements, email and chat session contents, and Web visits.

be installed on user computers for purposes that accrue to the commercial, financial, or personal interest of some third party.

- Adware, which can be illegal if not explicitly licensed for use on the user computer, tracks user Web behavior and targets specific pop-up ads based on the behavior profile and often comes as a surreptitious add-on (legally enabled through vague statements piggybacked in user license agreements) to popular peer-to-peer file sharing programs like KaZaa, Bearshare, and Limewire. Browser hijackers change the default web page setting on user browsers without permission, and may even make registry changes to prevent switching back to the preferred default homepage [Mikusch, 2003].
- Dialers are illegal programs that use a PC's modem to dial numbers that result in expensive toll charges for the user (and handsome kickbacks for the spyware owner), such as 900 numbers, expensive 10-10-xxx access code users, and overseas connections[Internet Journal, 2002].
- Drive-by downloads are spyware applications that install themselves on computers without user knowledge or consent during visits to Web sites. These applications can take almost any form from remote monitoring and reporting to actual Trojans with remote administration capabilities [Schwartz, Davidson and Steffan, 2003].
- So-called "scumware" changes website content by linking Web page keywords to the site of a third party [Daniels, 2004].
- A backdoor is a type of Trojan that allows a remote user full access to the machine at some later point. These remote control programs like Back Orifice or SMTP engines are often used by spammers as relays to send e-mail messages [Farrow, 2003];
- Other types of Trojans such as keystroke loggers and screen capture utilities simply watch, record, and report [Ferrer and Mead, 2003]. The most obvious purpose for this type of spyware is to capture credit card numbers, passwords, and other information that a remote user could use for various forms of identity theft.
- Web bugs are 1-pixel graphics or cookies that are used by websites to track an individual's computing behavior [Doyle, 2003]. They are often hidden in an HTML mail message (to identify if it has been read or not) and to place a cookie on a user's hard drive for future retrieval by the spyware. What makes web bugs particularly nasty is that even the most careful user can become a victim of a web bug simply by reading a message or viewing a web page.

II. WHY SPY?

Some spyware can be used legitimately, if not always ethically. Parents and managers can use keystroke loggers to monitor the Internet behavior of those they are responsible for [Ferrer and Mead, 2003], and businesses can use remote monitoring capabilities better to target the Internet browsing and shopping experience for users (e.g., [Naider, 2004; Wildstrom, 2004]). However, it is a short step from monitoring the Internet use patterns of a minor or an employee, to impersonally hacking a user's computer to record keystrokes that contain passwords and credit card numbers.

Businesses became interested in remote monitoring applications because of the dismal performance of banner ads in the online commerce world [Townsend, 2003]. Adware, which targets ads based on browsing habits, far surpasses the poor click-through rates on Internet banner ads, and carries the added benefit of being one of the few advertising media that can reach office workers at their desk [Townsend, 2003]. Business certainly cannot be faulted for wanting to get the best impact for their online promotional dollar, but even though there are

legitimate business models that depend on remote monitoring, the majority of spy threats faced by users have little legal basis for operation.

EXAMPLES

Contrasting Views

The consumer advocacy group Center for Democracy and Technology and the Business Software Alliance take contrasting views of spyware.

- To the Center for Democracy and Technology, spyware represents a widespread variety of computer applications that reside on users' computers and secretly connect to external Web sites to communicate personal information to outsiders [Berman, 2004]. Common among these applications is a lack of transparency and an absence of respect for users' ability to control their own computer and Internet connections.
- The Business Software Alliance (BSA), however, characterizes the spyware problem as more behavioral than technological (e.g., [Holleyman, 2004]). BSA states that applications often characterized as spyware (something that maintains a quiet back channel connection to an external site, in Gibson's [2003] view) are often used for business purposes by numerous companies seeking to provide more effective service to customers [e.g., Naider, 2004]).

Example: Microsoft

The archetypical example of this "improved customer service" application is the Microsoft Windows Update™ process, which upgrades and tries to improve various Microsoft applications on user computers via an Internet connection to Microsoft servers. Users are unaware that their computer was in communication with Microsoft servers until the operating system displays an "update available" message. The difference between this process and what typically happens with genuinely malicious spyware applications is that the Microsoft update process obtrusively notifies users that downloads are available and seeks permission for continuing the installation[2]. By contrast, many spyware applications would simply download and install software without a notification.

Example: Google

Google effectively uses Internet connectivity and user data reporting for business purposes [Wildstrom, 2004]. The Google Toolbar™ can be installed with a reporting function that allows Google to use your Internet browsing and search behavior to modify its services to you to be more useful personally. Many companies use reporting software similarly, though few are as forthcoming as Google.

Examples: RealNetworks and KaZaa

RealNetworks, for example, requires you to actively opt out of the installation of reporting software as part of its main installation. KaZaa slips in a brief notice about the Claria "Gator" adware product deep within its lengthy End User Licensing Agreement (EULA)[Wildstrom, 2004].

Example: Kodak

The authors experienced an unexpected installation of the remote monitoring and reporting application BackWeb Lite as part of the installation of Kodak digital camera software. BackWeb

[2] unless users have specifically and consciously chosen in response to a system prompt to have the updates handled automatically

is nominally a software update agent for the Kodak imaging application. However, we found that the agent installed numerous "hooks" into the target desktop computer's operating system and Internet applications. The resulting utilization of computer resources and Internet connectivity by the update agent degraded the computer's performance so noticeably that the computer owner felt compelled to perform a spyware scan to determine the cause of the performance degradation.

Discussion

Business applications, such as Windows Update™ and the Kodak update agent, are designed to "phone home" just like malicious spyware applications do, yet some of these legitimate business applications, if not well designed and integrated into the supported application, can cause noticeable computing delays when communicating to the home server, thereby aggravating the users they purport to be serving. In the Kodak case, this result could be caused by a lack of foresight in the choice on Kodak's part to graft off-the-shelf applications such as BackWeb Lite into their camera support applications as an update agent, rather than designing applications from scratch to integrate more effectively with the camera support software.

On the one hand, Microsoft's back channel update application is designed as a part of the operating system. The result is a degree of transparency that permits users to understand what the agent is doing. At the same time it is not overly invasive nor resource intensive. On the other hand, Kodak's back channel application is effectively covert as an installation since users have to look very closely in the EULA to even realize that an update agent is to be installed as part of the camera support package. Kodak's agent is maximally intrusive in its operation, given that the selected BackWeb agent consumes inordinate amounts of computer resources and bandwidth in what appears to be a constant dialogue with the Kodak server in search for application upgrades.

In the Kodak case, no overt harm was done since BackWeb Lite is not communicating personal information to Kodak from the user computer. However, the noticeable degradation in user computer performance is an issue that deserves consideration. We brought this issue to Kodak's attention, so future versions of their update agent may well be better integrated into the imaging support software. However, the apparent lack of respect for computer user resources on the part of businesses is the issue that results in applications such as Kodak's update agent being categorized together with more malicious and illegal uses of computer monitoring software.

Almost any application that actively communicates across the Internet, under Gibson's "back channel" definition [Gibson, 2003], can be a case of spyware in terms of its practical effect on user computing; the questions, then, are what sorts of uses was the application in question designed for, and why is it communicating to sites external to the computer it is installed on? What business practices underpin the desire on the part of some company or individual to install remote monitoring software on another individual's computer?

III. WHO USES SPYWARE, AND WHY?

Spyware can be used by anyone who wants to know something about another person's and his/her computing habits. As indicated in Sections I and II, the range of scenarios include parents or spouses keeping track of their family members or employers monitoring workers for appropriate Internet use, as well as the various illegal and illegitimate uses [Baldwin and Klingdon, 2003; Levine, 2004]. Businesses concerned with employee computer use, hackers seeking illegal gains, marketing organizations seeking to enlarge CRM databases for advertising and targeted selling purposes, the government, and even software publishers such as Microsoft fit this description. For example, Microsoft is known to track computer user music listening habits through the Windows Media Player application, when Internet enabled [Farrow, 2003]. The FBI's Carnivore program (since nominally dropped) is a case of spyware used legally in the name of national security [Ferrer and Mead, 2003].

COMMERCIAL USES

A primary legitimate business use for spyware is for marketing segmentation and audience targeting [Radcliff, 2004]. Businesses are increasingly making the use of spyware to gather valuable customer data as part of their mission [Foster, 2002], and it is becoming increasingly popular in e-business circles to use spyware as a means to gain additional revenues when operating in the online space.

Of these, a prominent recent example is Gator [Hagerty and Berman, 2003]. This software application provides bargain search utilities and e-Wallet services, which bring with them a surveillance package that serves to direct targeted advertising at user computers. Legally, the "clickwrap" EULA provides the legal cover for the installation of the bundled surveillance software. However, the claim of legal authorization through the EULA did not serve to protect Claria and other adware producers from trademark and copyright infringement suits arising from the placement of advertisements competing with e-commerce Web sites that users might visit. The Hertz rental car agency sued over pop-up ads promoting their competitors upon customer visits to Hertz, and copyright violation suits also are pending against Gator by Dow Jones and the Washington Post [Hagerty and Berman, 2003].

Pushy Registrations and Backchannel Updates

Some businesses use spyware-like applications for legitimate purposes, such as providing an active agent on customer computers to check for upgrades and to promote new software features [Anon, 2004]. Kodak's use of BackWeb Lite fits this well-intentioned, if not well-executed, scenario. Sometimes remote monitoring and reporting applications are used by companies for product activation, as with software sold by Quicken, Microsoft, and Macromedia. Along with simple product activation, the software can be used to force registration and subsequently collect information about the user for the vendor or software coder. This information can then be used for a variety of marketing purposes.

MALICIOUS USES

Hackers, it is feared, already employ spyware for many reasons, and are likely to do so more frequently in the future [Doyle, 2003; Radcliff, 2004]. Some hackers may use Trojans as a means of creating a network of compromised computers to use for a Distributed Denial of Service (DDoS) attack. Others may use the same means for creating a network of computers for delivering spam at a future date. Hackers may also use keystroke logging software to capture personal information, such as passwords and credit cards. The hackers may themselves then use this information for identity theft, or they may sell or trade this information with others so that they may commit similar acts.

IV. PROBLEMS ASSOCIATED WITH SPYWARE

Consumers loathe spyware for several reasons, not the least of these is the potential for invasion of privacy and the appropriation of personal information surreptitiously by unscrupulous marketers. The pop-up ads that spyware generate are rarely popular among the computer users targeted for their attentions. However, a more important issue is that spyware can interfere with the operation of computers, monopolizing CPU cycles and networking bandwidth.

APPROPRIATION OF COMPUTER RESOURCES

A company using spyware legally (through clickwrap agreement to a "carrier" application) or even in the case of a company seeking to use it for the most objective and positive reasons, often uses applications that are not extremely well-written, and that tend to interfere with users' computer functionality [Anon, 2004]. These applications tend to make lots of registry entries [Radcliff, 2004],

as in the case of Kodak and BackWeb Lite, where typical de-installation of the application with Spybot Search and Destroy,[3] results in the identification of nearly 60 registry entries. While the monitoring and reporting application can be removed from piggyback applications, registry alterations typically must be done manually, and can be tedious.

These monitoring and reporting applications generally run stealthily, so that the user is not able to detect them until prompted to investigate a degradation of system performance that occurs for no apparent reason. When a user has several instances of spyware running concurrently, the problem will magnify itself even more Moreover, as tricky as spyware is to detect, it may be even tougher to remove. Removing spyware may cause your Internet connection to fail if it alters the Winsock stack (e.g., [Foster, 2002]), and removing it may also cause other legitimate software (like the program that it piggybacked along with) to cease functioning correctly. All of the time and frustration encountered leads to serious costs for the users.

VIOLATION OF PRIVACY

Privacy invasion is a chilling concern. Some, like Sun Microsystems's Scott McNealy, told Internet users to ignore potential privacy violations, since privacy cannot be reasonably expected online [Wired News, 1999]. For most users, it is not so simple. The idea that someone out there is collecting personal information without our permission goes against basic tenets of liberty and freedom that are set out in documents like the U.S. Constitution; certainly, the parallels to the most potent privacy law applicable, the Federal wiretap statutes, are interesting and potentially applicable to unauthorized spyware installations [Farrow, 2003]. The threat of identity theft, once thought to be a minor annoyance, is a reality today. This crime is one of the fastest growing, and is expected by the Gartner Group to be even more prominent in the near future [Radcliff, 2004].

V. WHAT CAN YOU DO TO PROTECT YOUR PRIVACY? [4]

The leading culprit in spyware transmissions is the free Internet download of a software application. Notable examples of popular downloadable applications that carry spyware with them include Bonzi Buddy, Comet Cursor, and Gator [Coggrave, 2003]. as well as Xupiter Toolbar, Bargains.exe and a host of peer-to-peer applications that proliferated for music and video file sharing [Taylor, 2002]. If choosing to download applications from the Internet, you should be aware that the "clickwrap" licensing agreement that comes with such software generally will state (in rather unobvious ways) that the licensing company has the right to monitor use of the application or to collect personal information for certain purposes. Since a download will not proceed until "I Agree" is clicked on the license agreement, the download itself serves as evidence that you did give consent for the piggybacked spyware to be installed on their computer. This "licensed bundle" approach is the step that most companies take to ensure they are not prosecuted under the applicable statutes that would consider unauthorized installation of such spyware to be illegal. Hence, the best protection is:

- Do not download peer-to-peer application bundles,
- Avoid downloading any free software you are not familiar with, and
- Don't download software, even if you are familiar with it, if you are unwilling to fully examine the license before executing the download.

Expect that the true cost of "free" online is counted in the loss of privacy [Klang, 2003].

---

[3] A popular shareware spyware detection and removal tool found at http://www.safer-networking.org/

[4] In this section we address you, the reader, with the best advice we can give on how to defend yourself against spyware.

LOGICAL PROTECTIONS

The best way to avoid spyware is to be a cautious computer user and software consumer. Simply act on the presumption that

> *any software installation they undertake is likely at some specific level of probability to result in a surreptitious and associated spyware installation.*

This principle should be your working assumption as a spyware self-defense tactic for any commercial application you might consider installing. This assumption is an admittedly pessimistic view of the software industry, but the fact is that a robust and popular revenue model (cf. [Klang, 2003; Townsend, 2003]) strongly promotes the bundling of spyware with other "free" applications that you may want to download from the Internet. Producers of spyware applications will gladly pay commercial software producers who may feel that their products are not earning sufficient profits (free downloads are a good case in point) to bundle the spy application along with the desired shareware application that you might actively seek to install.

Since peer-to-peer (P2P) music sharing software is one of the most common spyware delivery modes, it may seem a matter of common sense to refuse to download and install popular file sharing applications. Yet, spyware downloads can also be triggered by Web site access, by using popular browsers that were not patched against vulnerabilities, by carelessly opening unexpected email attachments, or by not regularly and faithfully patching the numerous Microsoft operating system weaknesses as they continue to be identified [Levine, 2004]. Even so, the key threat remains the casual free software download, as part of an application bundle, that is not clearly or overtly disclosed, that is disguised, or that is actively hidden in the depths of extensive licensing agreements.

It is now a distinct possibility that computers can be delivered from the manufacturer with numerous spyware applications pre-installed as part of the OEM package (e.g., [Levine, 2004; Thompson, 2003]). Hence, as a normal computing practice, simply being aware of the current state of your computer and its various status lights, such as the ones indicating hard disk and network connection activity, is a good initial defense and signal of untoward malware in action [Rubenking, 2004]. Since spying applications generally exploit the computer's resources and networking connectivity to "phone home" with reports of user activity, unexpected disk or network activity is a clear warning of possible spyware activity. Thus, the second best way for you to avoid spyware problems is to:

- Maintain a high degree of awareness of your computer's operating state, and
- Integrate a spyware monitoring and sweeping program just as you have become accustomed to do with anti-virus measures.

To protect against spyware installed surreptitiously, or for those cases where you simply agreed to the license terms without reading the full text of the agreement, you can use one of numerous removal applications, some of which are also free. Spybot Search and Destroy (http://www.safer-networking.org/) is reported to be effective, and easier to use than the other alternative, Lavasoft's Ad-Aware (e.g., [Foster, 2002]). For the Mac user, the best alternative is considered to be the Spring Cleaning application, which is commercially available for around $50.00 [Taylor, 2002]. PestPatrol.com offers a commercial package that is scalable up to enterprise level for Windows users.

A third important step you can take is to inform yourself about spyware and its remedies. Among the wide variety of resources available are:

- Spyware Guide [2004] and GRC.com [Gibson, 2003], which provide handy guidelines for how to protect your computer from malicious intrusions,

- Spyware Labs [2004] which investigates how companies can use spyware in an economic fashion. This company also publishes a shareware spyware detector, Virtual Bouncer, and they publish Spyware Quarterly, and
- PC Magazine [e.g., [Metz, 2004; Rubenking, 2004]) ran a detailed review of spyware detection and removal tools. This review is not only informative about the spyware problem, but highly useful in identifying a full range of fee-based and shareware solutions, all tested, rated, and evaluated by the magazine's staff.

LEGAL PROTECTIONS

A close reading by users of clickwrap license agreements for "free" software downloads and applications is an essential legal protection against many remote monitoring programs that might be an instance of spyware. The "EULA Defense" is still, to this day, generally held by Federal courts as technical legal justifications for software installation [cf., Berman, 2004; Bruening and Steffen, 2004; Klang, 2003; Townsend, 2003; Urbach and Kibel, 2004]. This "quick-trick" method of legally installing remote monitoring software onto user computers will likely continue as long as directly served pop-up ads triggered by adware continue to return significantly better click-through results than banner ads on Web sites [Klang, 2004; Urbach and Kibel, 2004], and as long as Federal courts continue to recognize the EULA defense as technically meeting the letter of the law.

Privacy is clearly the price paid for "free" software downloaded from the Internet, There is some question as to whether the transaction is a fair one, since under contract theory both parties to an agreement are presumed to be fully informed and fully in agreement on all of the terms [Klang, 2004]; yet, this assumption is not true in most bundled adware downloads. A prevailing legal point is that incidental trespass on a user's computer arises from connection to the Internet; the Internet is a door that users opened, and, as long as the adware installed does not harm the user's computer, the incidental trespass is harmless [Volkmer, 2004]. This same principle of material effect was used in the past to defend spammers successfully against charges of trespass to chattel. Privacy advocates are emphatic that the minimal notice currently provided as legal cover for an adware download does not provide consumers with the requisite degree of notice and choice. This shortcoming probably gives the FTC the power to regulate the practice on the basis of deceptiveness and fairness provision of Title 5 of the FTC act [Berman, 2004; Levine, 2004].

The other approach to legal remedies is to change the law. The spyware issue came to the attention of the U.S. Congress in 2000, when Senator John Edwards of North Carolina first introduced his proposed anti-spyware legislation. Neither of Senator Edwards' proposals [Edwards, 2000; 2001] was brought to a vote. In the 108th Congress, Senators Conrad Burns of Montana, Ron Wyden of Oregon, and Barbara Boxer of California introduced S. 2145, the SPYBLOCK Act (Software Principles Yielding Better Levels of Consumer Knowledge), seeking to prohibit the installation of software on computers without notice and consent, and requiring reasonable uninstall procedures for all downloadable software [O'Shea, 2004]. This legislation attained prominent notice in committee (e.g., [U.S. Senate Committee on Commerce, Science and Transportation, 2004]). U.S. Congresswoman Mary Bono of California introduced the Safeguard Against Privacy Invasions Act in the House of Representatives [Volkmer, 2004], which passed the House Energy and Commerce Subcommittee in 2004[Urbach and Kibel, 2004].

These measures, both in and out of committee, generated considerable attention in the legal community, as evidenced by coverage in the legal literature (cf., [Bruening and Steffen, 2004; Klang, 2003; Urbach and Kibel, 2004; Volkmer, 2004]) and recent high-profile hearings in the Federal regulatory bureaucracy (e.g., [Beales, 2004]). Hence, in addition to logical steps users can take to avoid spyware infestations, Federal laws may eventually provide some legal prevention from unwarranted software intrusions.

V. CONCLUSION

As was the case with e-mail spam in recent years, once a technique is demonstrated for exploiting the Internet as a commercial tool, or as an aid to fraud, the usage of the technique only increases. We can likely expect far more creative spyware attacks on user privacy in the future, together with increasing numbers of legal commercial applications developed for customer relationship management purposes. Awareness of the threats posed by both legal and illegal applications of spyware technology is the best protection, since the nature of the threat to computer users will naturally evolve over time.

This paper catalogs not only the range of potential threats and harms of spyware technology, but also lists a number of solutions and resources for user protection. We believe that the routine sweeping of computers for spyware will become a standard weekly practice that will take place right alongside the virus checks prudent computer users became used to in recent years. A number of tools are identified here for that purpose.

The emerging legal issues related to the spyware problem are also identified. Details are provided on the various legislative initiatives underway to prevent, regulate, and punish improper spyware use. The problem associated with this approach to the spyware problem is that there is likely to be little agreement among legislators, citizens, and businesses about what actually constitutes a regulatory instance of spyware, nor which sorts of programs should be regulated [Berman, 2004; Holleyman, 2004; Thompson, 2003]. This challenge is typical in legislative and regulatory processes. The conflicting interests of numerous constituencies are modified through compromise and reconciliation [Beales, 2004; Prostic, 2004]. Moreover, these legal remedies are likely to be quite slow in coming, as is also typical of the legislative process. At this point, regardless of the activities in the U.S. Congress, the only legislation actually to be enacted to control spyware exists at the state level, in Utah [Urbach and Kibel, 2004].

As we await the results of regulatory scrutiny and bureaucratic investigation, it would be useful to begin:

- Documenting the impact of spyware,
- Investigating and describing consumer reactions and business concerns, and
- Assessing user sensitivity to the sorts of potential intrusions that are engaged in by various spyware applications.

Such knowledge would advance the general understanding of the spyware problem, while providing the empirical documentation necessary to support effective regulation of the problem [e.g., Beales, 2004].

A RESEARCH AGENDA

Little empirical work supports the many suppositions being made about spyware and its effects on personal and business computing [Beales, 2004]. As with any topic of scholarly inquiry, the recognition of a problem is just the first step in investigating its causes and cures. This paper begins the process for the spyware problem. The legal and legislative solutions to the problem are actively under consideration, as amply demonstrated here. However, the only real published research on the spyware problem in mid-2004 is what appears in law journals (cf., [Bruening and Steffen, 2004; Klang, 2003; Urbach and Kibel, 2004; Volkmer, 2004]).

The following subsections synthesize the spyware literature and develop a research agenda for work that needs to be done.

Step One: Describe the Problem

The first step in dealing with spyware is to understand it. This step requires descriptive research that catalogs:

- The range and variety of intrusive applications that exist, and
- Frameworks for pigeonholing spyware by its attributes.

Once done:

- Practitioners would know what their software legally can and cannot do with and to a user's machine and where the line is for system aid vs. system hindrance,
- Users would know which applications to avoid, simply by knowing which applications are capable of undesirable monitoring activity,
- Lawmakers would have a tested, active framework to use when regulating spyware, hence minimizing legal loopholes[5], and
- Classifications characterize degree of harm versus amount of help. Classification schemes would provide researchers a common base from which to start their analyses and would build towards theory development (e.g., [Kuhn, 1970]). Scholars would also know what sorts of applications are most relevant and hence deserve the greatest attention (e.g., [Benbasat and Zmud, 1999]).

Step Two: Understand End User Attitudes and Requirements

As with any good information system initiative, understanding computer user perspectives is vital. After completion of a framework, researchers then can begin the testing process. Accurate definitions and uses of various software packages can be provided to end users when profiling them through focus groups, surveys, or other data collection mechanisms. Existing research instruments can be adopted for use in specific spyware scenarios.

As the government begins to take a more active role in regulatory oversight of spyware applications, the perceptions of end users will be all the more important. The key mechanisms through which agencies such as the FTC can and will regulate intrusive applications and privacy violations involve the definitions of fairness and deception, which are relevant in context to end user perceptions about specific applications.

Step Three: Track Legislative and Regulatory Activity

An ongoing catalog of congressional activity and statutorily regulatory agencies is necessary. As outlined at the end of Section IV, laws and regulations about spyware are rudimentary and little progress is being made. Since the content of legislation currently under debate is likely to define the nature of spyware formally and to regulate it (e.g., [Berman, 2004]), spyware research programs need to stay abreast of legislative events.

Step Four: Profile User Segments

Not every computer user insists that the applications described here must be removed from his or her computer. For example, much of the intent of businesses in creating adware is ostensibly to support a greater range of consumer choice and convenience (e.g., [Naider, 2004]). Parts of the computer user marketplace is interested in adware applications that monitor user activity and direct targeted advertising to the desktop based on such activities[6],

---

[5] We assume that lawmakers prefer to help users rather than spyware vendors. This assumption may not be valid if large amounts of lobbying money are spent.

[6] An example is the case of the prominent technology writer who prefers to let the Google Toolbar™ application actually monitor and report back to Google on his activities in order to custom-tailor the search utility to his specific needs (e.g., [Wildstrom, 2004]). This case is a finely focused example of targeted marketing, and consumers interested in savings and convenience are certain to have interests that coincide with some adware providers.

A "bargain conscious" segment of computer users might directly correspond to the business models engendered by adware vendors such as WhenU.com (e.g., [Naider, 2004]). This segment of users will likely welcome, rather than wish to avoid, competitive pop-up ads that appear during online shopping sessions and Web searches for product information. Conversely, it is also likely that some user segments will jealously guard personal privacy and consider any remote monitoring application, no matter how legal, to be an offensive intrusion. Profiling characteristics of such segments will aid scholars and practitioners alike, in understanding the likely reactions to spyware applications by various user groups.

Final Thoughts

Spyware regulation is in its infancy [Thompson, 2003]. We are only beginning to understand the problem, and must continue regularly to assess the influence, effects, and controls of spyware. Spyware is simply one more mechanism in the fight between users trying to protect their personal data and those who would try to use that data for exploitation. Where the inquisitive individual or business once needed to talk to the town gossip or perhaps dig through the target's trash to learn private information about others, they can now simply gather information through spyware. How society will treat, regulate, and assess spyware (perhaps even accept it) remains to be determined. Ongoing inquiry into spyware will lead to a better understanding of the issues, actions and consequences of this new class of software in society.

Editor's note: This article is based on a tutorial presented by the authors at AMCIS 2004. The article was received on August 3, 2004 and was published on September 7, 2004.

REFERENCES

EDITOR'S NOTE: The following reference list contains the address of World Wide Web pages. Readers who have the ability to access the Web directly from their computer or are reading the paper on the Web, can gain direct access to these references. Readers are warned, however, that

> 1. these links existed as of the date of publication but are not guaranteed to be working thereafter.
>
> 2. the contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.
>
> 3. the authors of the Web pages, not CAIS, are responsible for the accuracy of their content.
>
> 4. the author of this article, not CAIS, is responsible for the accuracy of the URL and version information.

Anonymous (2004), "Spyware: Spycatcher" *New Media Age*, January 8, p. 25.

Baldwin, R.W. and K.W. Klingdon (2003), "*Survey of Spyware and Countermeasures,"* Palo Alto, CA: Plus Five Consulting, Inc., http://www.plusfive.com/reports.html , accessed 7/12/04.

Beales, J.H. (2004), "Remarks of J. Howard Beales, Director, Bureau of Consumer Protection, *FTC Spyware Workshop, April 19, 2004,* http://www.ftc.gov/bcp/workshops/spyware/index.htm , current July 20, 2004.

Benbasat, I., and R. Zmud (1999), "Empirical Research in Information Systems: The Practice of Relevance," *MIS Quarterly*, (23)1, pp.3-16.

Berman, J. (2004), "Prepared Statement of Jerry Berman, President, The Center for Democracy and Technology," U.S. Senate Committee on Commerce, Science and Transportation, http://commerce.senate.gov/pdf/ berman032304.pdf (current July 14, 2004).

Bruening, P. J. and M. Steffen (2004), "Spyware: Technologies, Issues, and Policy Proposals," *Journal of Internet Law,* (7)9, pp.3-8.

Carfarchio, P. (2002), "The Challenge of Non-Viral Malware," PestPatrol White Paper, http://www.pestpatrol.com/Whitepapers/NonViralMalware0902.asp (current July 17, 2004).

CDT (2004), "Join CDT's Campaign against Spyware," http://www.cdt.org/ action/spyware/ (current July 16, 2004).

Coggrave, F. (2003), "How to Tackle the Spyware Threat," *Computer Weekly,* November 18. p. 30.

Daniels, J. (2004), "Scumware.biz Educates about Dangers of Adware/Scumware," *Computer Security Update,* (5)2,

Doyle, E. (2003), "Not All Spyware is as Harmless as Cookies: Block it or Your Business Could Pay Dearly," *Computer Weekly,* November 25, p. 32.

Edwards, J. (2000)," Senator Edwards Proposes Spyware Law," http://www.senate.gov/~edwards/press/2000/oct05-pr.html , (current July 29, 2004)

Edwards, J. (2001), "Senator Edwards Proposes Spyware Law," http://www.senate.gov/~edwards/press/2001/jan29c-pr.html (current July 16, 2004).

Electronic Privacy Information Center (EPIC) (2001), "Alert 8.03," http://www.epic.org/alert/EPIC_Alert_8.03.html (current July 16, 2004).

Farrow, R. (2003), "Is your Desktop being Wiretapped?" *Network Magazine,* (18)8, p. 52.

Ferrer, D. and M. Mead (2003), "Uncovering the Spy Network," *Computers in Libraries,* (23)5, p. 16.

Fisher, D. (2004), "New Cracks for IT Holes," *eWeek*, (21) 27, pp. 9-10.

Foster, E. (2002), "The Spy Who Loves You," *Infoworld*, (24)20, p. 60.

Gibson, S. (2003), "OptOut," http://www.grc.com/oo/news.htm (current July 17, 2004).

Hagerty, J. and D. Berman (2003), "Caught in the Net: New Battleground over Web Privacy: Ads that Snoop," *Wall Street Journal*, August 27, p. A1.

Holleyman, R. (2004), "The Testimony of Mr. Robert Holleyman, President and CEO, Business Software Alliance," U.S. Senate Committee on Commerce, Science and Transportation, http://commerce.senate.gov/ hearings/testimony.cfm?id=1125&wit_id=3166 (current July 14, 2004).

Intranet Journal (2002), "Inside Spyware: A Guide to Finding, Removing and Preventing Online Pests," http://www.intranetjournal.com/spyware (current July 17, 2004).

Klang, M. (2003), "Spyware: Paying for Software With our Privacy," *International Review of Law, Computers & Technology*, (17)3, pp.313-322.

Kuhn, T. (1970). *The Structure of Scientific Revolutions*. Chicago, IL: University of Chicago Press.

Levine, J.R. (2004), "Written Comments of Dr. John R. Levine," U.S. Senate Committee on Commerce, Science and Transportation, http://commerce.senate.gov/pdf/levine032304.pdf (current July 14, 2004).

Metz, C. (2004), "Spy Stoppers," *PC Magazine*, March 2, www.pcmag.com/print_article/0,1761,a=118675,00.asp (current April 28, 2004).

Mikusch, R. (2003), "Adware, Spyware – Oh My!" *Beyond Numbers*, (427)October, 16.

Naider, A.V. (2004), "Testimony of Mr. Avi Z. Naider," U.S. Senate Committee on Commerce, Science and Transportation, http://commerce.senate.gov/ pdf/naider032304.pdf (current July 14, 2004).

O'Shea, J. (2004), "Burns Introduces Spyware Bill," http://burns.senate.gov/ index.cfm?FuseAction=PressReleases.View&PressRelease_id=1077 (current July 16, 2004).

Prostic, E. (2004), ""Remarks of Elizabeth Prostic, Chief Privacy Officer, United States Department of Commerce," *FTC Spyware Workshop, April 19, 2004,* http://www.ftc.gov/bcp/workshops/spyware/index.htm , current July 20, 2004.

Radcliff, D. (2004), "Spyware," *Network World,* (21)4, p. 51.

Rubenking, N.J. (2004), "11 Signs of Spyware," *PC Magazine*, March 2, www.pcmag.com/print_article/0,1761,a=118675,00.asp (current April 28, 2004).

Schultz, E. (2003), "Pandora's Box: Spyware, Adware, Autoexecution, and NGSCB," *Computers & Security*, (22)5, p.366.

Schwartz, A, A. Davidson and M. Steffan (2003), "Ghosts in Our Machines: Background and Policy Proposals on the "Spyware" Problem," Washington, D.C.: Center for Democracy and Technology, http://www.cdt.org/action/spyware/ (current July 16, 2004).

Spyware Guide (2004). http://www.spywareguide.com (current July 14, 2004).

Spyware Labs (2004). http://www.spywarelabs.com/research.html (current July 14, 2004).

Taylor, C. (2002), "What Spies Beneath," *Time*, (160)15, p. 106.

Thompson, R. (2003), "Cybersecurity & Consumer Data: What's at Risk for the Consumer?" Testimony before the U.S. House of Representatives Subcommittee on Commerce, Trade, and Consumer Protection, http://www.iwar.org.uk/comsec/resources/consumer-risk/ Thompson1799. htm (current July 7, 2004).

Townsend, K. (2003), "Spyware, Adware and Peer-to-Peer Networks: The Hidden Threat to Corporate Security," PestPatrol White Paper, http://www.pestpatrol.com/Whitepapers/CorporateSecurity0403.asp (current July 17, 2004).

Urbach, R.R. and G.A. Kibel (2004), "Adware/Spyware: An Update Regarding Pending Litigation and Legislation," *Intellectual Property & Technology Law Journal*, (16)7, pp. 12-16.

U.S. Senate Committee on Commerce, Science and Transportation (2004), "Spyware: Communications Hearings," http://commerce.senate.gov/hearings/witnesslist.cfm?id=1125 (current July 14, 2004).

Volkmer, C.J (2004), "Should Adware and Spyware Prompt Congressional Action?" *Journal of Internet Law*, (7)11, pp. 1-8.

Waterfield, P. (2004). *New Weapons in the War Against Spyware, Adware and P2P File Sharing*. Boston, MA: Yankee Group.

Wildstrom, S.H. (2004), "How to Stymie the Snoop in Your PC," *BusinessWeek,* April 5, p. 28.

Wired News (1999), "Sun on Privacy: Get Over It," http://www.wired.com/news/politics/0,1283,1753 8,00.html (current February 20, 2004).

ABOUT THE AUTHORS

Tom Stafford is Assistant Professor of Management Information Systems at the University of Memphis. Dr. Stafford holds a Ph.D. in MIS from the University of Texas – Arlington and a Ph.D. in Marketing from University of Georgia. His research spans the topics of e-business, e-commerce, supply chain management, and motivations for Internet use. His work is published in

Communications of the ACM, *Decision Sciences*, and *IEEE Transactions on Engineering Management*, among others

Andrew Urbaczewski is Assistant Professor of Management Information Systems at the University of Michigan – Dearborn. He received a Ph.D. in Information Systems from Indiana University, an MBA from West Virginia University, and a BS in Finance (with honors) from the University of Tennessee. His research interests include wireless mobile collaboration, electronic commerce, and electronic monitoring of employees. His research is published in *the Journal of Management Information Systems, Communications of the ACM*, *Journal of Organizational Computing and Electronic Commerce*, and *Communications of the AIS*, among others.