Anti-Spyware Coalition
Definitions and Supporting Documents

Spyware has quickly evolved from an online nuisance to one of the most dire threats facing the Internet. As users struggle to maintain control over their computers, many find themselves trapped in a cyclical battle against programs that install themselves without warning, open dangerous security holes and reinstall themselves after they've been deleted. The worst of these programs allow online criminals to hijack users' sensitive personal information at will. Even the most benign variants can slow computers to a crawl by wasting their processing power to provide unwanted "services." Compounding the problem are the sophisticated ploys spyware developers use to install their programs on unsuspecting users' computers. Spyware distributors often rely on security holes, clever cons, opaque "bundling" arrangements and other unsavory practices to spread their unwanted payload. As the threat has grown, so has the need to mount a coordinated defense against these unwanted programs and their adverse effects.

The Anti-Spyware Coalition was convened to bolster that defense, by building on the great strides the technology industry has already made to combat the spyware problem. In recent years, computer and software makers have taken serious steps to safeguard their products and to educate consumers about how to avoid falling victim to spyware. At the same time, a strong and growing anti-spyware industry has created an array of tools to help consumers identify and purge their computers of unwanted technology. The Anti-Spyware Coalition is made up of public interest groups, trade associations and the most prominent anti-spyware companies and their distributors. Drawing on the combined expertise of its membership, the coalition is working to identify common definitions, tools and practices that will improve the effectiveness of anti-spyware technology and help consumers better understand how those tools work to defend them. The following documents represent the completion of first phase of that process. Coalition members felt it vital to establish common definitions of spyware and other potentially unwanted technologies so that vendors, software developers and consumers could better communicate about what sorts of technologies raise concerns, and how anti-spyware programs identify potentially unwanted programs. Included below are:

- A, simple, formal definition of *Spyware and Other Potentially Unwanted Technologies* a term the coalition uses to define the panoply of technologies that may impinge a user's computing experience, privacy, or security.

- A comprehensive *Glossary* that offers clear definitions for terms commonly used in discussions about spyware and other potentially unwanted technologies.

- A set of common industry guidelines for the *Vendor Dispute Resolution Process.* This document outlines the steps that anti-spyware companies should take in responding to complaints from software publishers who allege that their software has been improperly flagged as "spyware."

- Finally, the *Anti-Spyware Safety Tips* offer basic guidance for consumers to protect themselves and their computers.

These documents are working drafts that will serve as the cornerstone of the Anti-Spyware Coalition's ongoing efforts. They lay the foundation for the ongoing and future work of the

coalition . The documents will evolve as new problems are identified and our understanding deepens. We continue to invite public input on all of our public documents as we proceed.

About the AntiSpyware Coalition

The ASC is a group dedicated to building a consensus about definitions and best practices in the debate surrounding spyware and other potentially unwanted technologies. Composed of anti-spyware software companies, academics, and consumer groups, the ASC seeks to bring together a diverse array of perspective on the problem of controlling spyware and other potentially unwanted technologies.

Current ASC Members

- Aluria
- AOL
- Blue Coat Systems
- Canadian Coalition Against Unsolicited Commercial Email
- Canadian Internet Policy and Public Interest Clinic
- Center for Democracy & Technology
- Computer Associates
- CyberSecurity Industry Alliance
- Dell, Inc.
- EarthLink
- F-Secure Corporation
- HP
- ICSA Labs
- LANDesk
- Lavasoft
- McAfee Inc.
- Microsoft
- National Center for Victims of Crime
- Panda Software
- PC Tools
- Safer-Networking Ltd.
- Samuelson Law, Technology & Public Policy Clinic at Boalt Hall, UC Berkeley School of Law
- Sophos
- Symantec
- Tenebril
- Trend Micro
- Webroot Software
- Websense
- Yahoo! Inc.

The Center for Democracy and Technology coordinates]the Anti-Spyware Coalition. Anti-spyware companies or public interest groups interested in joining the Coalition should contact Ari Schwartz, CDT Associate Director at asc@cdt.org or at 202-637-9800.

Spyware and Other Potentially Unwanted Technologies

Technologies deployed without appropriate user consent and/or implemented in ways that impair user control over:

- Material changes that affect their user experience, privacy, or system security;
- Use of their system resources, including what programs are installed on their computers; and/or
- Collection, use, and distribution of their personal or other sensitive information.

Examples of Spyware and Potentially Unwanted Technologies

The table below lists some technologies that have been used to harm or annoy computer users. It is important to note that with proper notice, consent, and control some of these same technologies can provide important benefits: tracking can be used for personalization, advertisement display can subsidize the cost of a product or service, monitoring tools can help parents keep their children safe online, and remote control features can allow support professionals to remotely diagnose problems.

For example, the underlying technology that enables a keylogger is Tracking Software. Tracking Software can both harm and help a user. When a keylogger is installed and executed covertly, it is spying. On the other hand, a keylogger can be used for legitimate purposes with clear consent, such as letting an IT help desk remotely assist a user in problem diagnosis. Underlying technology typically becomes unwanted when it is implemented in a way that provides no benefit to -- or actively harms -- authorized users.

Common Terms for Well-Known Unwanted Varieties	Underlying Technology	Description of Underlying Technology	Why the Underlying Technology May Be Unwanted	Why the Underlying Technology May Be Wanted
• Spyware (narrow)* • Snoopware • Unauthorized Keylogger • Unauthorized Screen Scraper	Tracking Software	Used to monitor user behavior or gather information about the user, sometimes including personally identifiable or other sensitive information.	• Done covertly, tracking is spying • May collect personal information that can be shared widely or stolen, resulting in fraud or ID theft • Can be used in the commission of other crimes, including domestic violence and stalking • Can slow machine down • May be associated with security risks and/or loss of data	• May be used for legitimate monitoring: e.g. by parents or companies • May be a necessary component of adware that is linked to wanted software • May allow customization
Nuisance or Harmful Adware	Advertising Display Software	Any program that causes advertising content to be displayed.	• May be a nuisance and impair productivity • May display objectionable content • Can slow machine down or cause crashes and loss of data • May not provide users with adequate removal tools • May be associated with security risks	• May be linked to other software or content that is wanted, subsidizing its cost. • May provide advertising that is desired by the user.

Examples of Spyware and Potentially Unwanted Technologies (continued)

Common Terms for Well-Known Unwanted Varieties	Underlying Technology	Description of Underlying Technology	Why the Underlying Technology May Be Unwanted	Why the Underlying Technology May Be Wanted
• Backdoors • Botnets • Droneware	Remote Control Software	Used to allow remote access or control of computer systems	• Can be used to turn a user's machine into a mass mailer or soldier for DDoS attack or a host for malicious or inappropriate content • Done covertly, it is stealing cycles and other resources • Can slow machines down • May be associated with loss of data • May cause personal information to be shared widely or allow it to be stolen	• May allow remote technical support or troubleshooting • Can provide users remote access to own data or resources
Unauthorized Dialers	Dialing Software	Used to make calls or access services through a modem or Internet connection	• May cause unexpected toll calls to be made and charged to the user	• May allow access to desired services
• Hijackers • Rootkits	System Modifying Software	Used to modify system and change user experience: e.g. home page, search page, default media player, or lower level system functions	• Without appropriate consent, system modification is hijacking • Can compromise system integrity and security • Can drive user to spoofed web sites in order to steal their ID.	• May be used for desirable customization
Hacker Tools (including port scanners)	Security Analysis Software	Used by a computer user to analyze or circumvent security protections	• Are frequently used nefariously • Presence may violate corporate policies or family understandings	• Can be used for security research and other legitimate security purposes
Tricklers	Automatic Download Software	Used to download and install software without user interaction	• May be used to install unauthorized applications including those in the categories above	• May be used for automatic updates, or other automatic system maintenance
Unauthorized Tracking Cookies	Passive Tracking Technologies	Used to gather limited information about user activities without installing any software on the user's computers	• May allow unwanted collection of information (for example, Web sites a user has visited)	• May be used for desired customization or personalization (example: "similar items you might like") • May allow advertisers to avoid showing the same ad too often to the same person.

**See attached Glossary for a detailed discussion of various uses of the term "spyware."*

Glossary

ASC includes the following Glossary in order to clarify some of the terms used in this document, particularly the more frequently used terms in anti-spyware products and research. This Glossary will be updated as we continue with our work.

ActiveX Control: See "Browser Plug-in."

Advertising Display Software: Any program that causes advertising content to be displayed.

Adware: A type of *Advertising Display Software*, specifically certain executable applications whose primary purpose is to deliver advertising content potentially in a manner or context that may be unexpected and unwanted by users. Many adware applications also perform tracking functions, and therefore may also be categorized as *Tracking Technologies*. Some consumers may want to remove Adware if they object to such tracking, do not wish to see the advertising caused by the program, or are frustrated by its effects on system performance. On the other hand, some users may wish to keep particular adware programs if their presence subsidizes the cost of a desired product or service or if they provide advertising that is useful or desired, such as ads that are competitive or complementary to what the user is looking at or searching for.

Alternate Data Stream: An extension to Microsoft's Windows NT File System (NTFS) that provides compatibility with files created using Apple's Hierarchical File System (HFS). Applications must write special code if they want to access and manipulate data stored in an alternate stream. Some spyware uses these streams to evade detection.

Automatic Download Software: Any program used to download and install software without user interaction

Backdoor: A type of *Remote Control Software* that enables a third party to covertly control system resources.

Botnet: A type of *Remote Control Software*, specifically a collection of software robots, or "bots", which run autonomously. A botnet's originator can control the group remotely. The botnet is usually a collection of zombie machines running programs (worms, trojans, etc.) under a common command and control infrastructure on public or private networks. Botnets have been used for sending spam remotely, installing more spyware without consent, and other illicit purposes.

Browser Helper Object (BHOs): see "Browser Plug-in."

Browser Plug-in: A software component that interacts with a Web browser to provide capabilities or perform functions not otherwise included in the browser. Typical examples are plug-ins to display specific graphic formats, to play multimedia files or to add toolbars which include searching or anti-phishing services. Plug-ins can also perform potentially unwanted behaviors such as redirecting search results or monitoring user browsing behavior, connections history, or installing other unwanted software like nuisance or harmful adware. Types of Browser plug-ins include:

- **ActiveX controls:** A type of Browser Plug-in that is downloaded and executed by the Microsoft Internet Explorer Web browser.
- **Browser Helper Object (BHOs):** A Type of Browser Plug-in that is executed each time the Microsoft Internet Explorer Web browser is launched. Toolbars are a common form of BHO.
- **Mozilla Firefox Extensions:** A Browser Plug-in specific to Mozilla Firefox.

Bundling: The practice of distributing multiple pieces of software together, so that when the software "bundle" is installed, multiple components may be installed. In many cases, bundling is a convenient way to distribute related pieces of software together. However, in some cases, unwanted software

components, such as nuisance or harmful adware, can be bundled with programs users want, and can thereby be downloaded onto their computers without notice or consent.

Cookie: A piece of data that a Web site -- or a third party that was commissioned or approved by the website -- saves on users' computers' hard drives and retrieves when the users revisit that Web site. Some cookies may use a unique identifier that links to information such as login or registration data, online "shopping cart" selections, user preferences, Web sites a user has visited, etc. (See also Tracking Cookies.)

Dialer: Dialer is a colloquial term for *Dialing Software*.

Dialing Software: Any program that utilizes a computer's modem to make calls or access services. Users may want to remove dialers that dial without the user's active involvement, resulting in unexpected telephone charges and/or cause access to unintended and unwanted content.

Distributed Denial-of-Service (DDoS) Attack: A means of burdening or effectively shutting down a remote system by bombarding it with traffic from many other computers. DDoS attacks are often launched using the compromised systems of Internet users, often using botnets. An attacker will exploit a vulnerability in one computer system and make it the DDoS "master" using *Remote Control Software*. Later, the intruder will use the master system to identify and manage zombies that can perform the attack.

Downloader: A program designed to retrieve and install additional files. Downloaders can be useful tools for consumers to automate upgrades of essential software such as operating system upgrades, browsers, anti-virus applications, anti-spyware tools, games and other useful or enjoyable applications of all kinds. Automated upgrades are useful for closing off security vulnerabilities in a timely way. Unauthorized downloaders are used by third parties to download potentially unwanted software without user notification or consent.

Drive-by-Download: The automatic download of software to a user's computer when she visits a Web site or views an html formatted email, without the user's consent and often without any notice at all. Drive-by-downloads are typically performed by exploiting security holes or lowered security settings on a user's computer.

Droneware: Programs used to take remote control of a computer and typically used to send spam remotely, run DDOS attacks or host offensive Web images. See also "Botnet."

End User License Agreement (EULA): An agreement between a producer and a user of computer software that specifies the terms of use putatively agreed to by the user. The software producer specifies the parameters and limitations on use, which comprise a legally binding contract. Some companies use the EULA as the sole means of disclosure of a program's behavior (including bundling, use of the user's data, etc.).

Exploit/Security Exploit: A piece of software that takes advantage of a hole or vulnerability in a user's system to gain unauthorized access to the system.

Hacker Tool: *Security Analysis Software* that can be used to investigate, analyze or compromise the security of systems. Some Hacker Tools are multi-purpose programs, while others have few legitimate uses.

Hijacker: *System Modification Software* deployed without adequate notice, consent, or control to the user. Hijackers often unexpectedly alter browser settings, redirect Web searches and/or network requests to unintended sites, or replace Web content. Hijackers may also frustrate users' attempts to undo these changes, by restoring hijacked settings upon each system start.

Host File: A file, stored on the user's computer, used to look up the Internet Protocol address of a device connected to a computer network. Some spyware has been known to change a host file in order to redirect users from a site that they want to visit to sites that the spyware company wants them to visit.

Keylogger (or Keystroke Logger): *Tracking Software* that records keyboard and/or mouse activity. Keyloggers typically either store the recorded keystrokes for later retrieval or they transmit them to the remote process or person employing the keylogger. While there are some legitimate uses of keyloggers, but they are often used maliciously by attackers to surreptitiously track behavior to perform unwanted or unauthorized actions included but not limited to identity theft

Objective Criteria: The behavioral factors by which anti-spyware companies use to decide whether to consider a process or program is spyware.

Packer: A program that can compress and/or encrypt an executable file in a manner that prevents matching the memory image of that file and the actual file on disk. Sometimes used for copy protection, packers are often used to make spyware less easy to analyze/detect.

Passive Tracking Technologies: Technologies used to monitor user behavior or gather information about the user, sometimes including personally identifiable or other sensitive information.

Password Cracker: *Security Analysis Software* designed to allow someone to recover or decrypt lost, forgotten or unknown passwords. Password Cracker can guess a password by running a brute-force attack, e.g. testing each character combination to find the right password, or by running a dictionary attack, e.g. testing common words from large dictionaries, which could be used as password by users. While they can be a legitimate tool used by security administrators and law enforcement officers, Password Crackers pose a significant security and privacy threat when used illicitly.

Port Scanner: *Security Analysis Software* used to discover what computer network services a remote system provides. Port scanning indicates where to probe for weaknesses.

Privacy Policy: A legally binding notice of how a company deals with a user's personal information. The privacy policy should contain information about collecting information and the secondary uses of data, including how information is shared with third parties and who those third parties are.

Privilege Elevation: A process that allows an individual or device to gain unauthorized privileges, usually administrator level access, on a computer or network.

Registry: A database integrated into certain operating systems which store information, including user preferences, settings and licence information, about hardware and software installed on a user's computer.

Registry Keys: The individual entries in the registry. The value of the keys is changed every time a new program is installed or configuration settings are modified. Spyware often changes registry key values in order to take control of parts of the system. These changes can impair the regular function of the computer.

Remote Access/Administration Tool (RAT): An executable application designed to allow remote access to or control of a system. RATs are a type of *Remote Control Software.* While there are many legitimate uses of RATs, they can be used maliciously by attackers to start or end programs, install and uninstall new software, or perform other unwanted or unauthorized actions.

Remote Control Software: Any program used to allow remote access or control of computer systems.

Risk Modeling: The process used by anti-spyware vendors to determine the categorization of spyware, both in terms of level and type of risk.

Rootkit: A program that fraudulently gains or maintains administrator level access that may also execute in a manner that prevents detection. Once a program has gained access, it can be used to monitor traffic and keystrokes; create a backdoor into the system for the hacker's use; alter log files; attack other machines on the network; and alter existing system tools to circumvent detection. Rootkit commands replace original system command to run malicious commands chosen by the attacker and to hide the presence of the Rootkit on the system by modifying the results returned by suppressing all evidence of the presence of the Rootkit. Rootkits are an extreme form of *System Modification Software*.

Screen Scrapers/Screen Capturers: *Tracking Software* that records images of activity on the screen. Screen Scrapers typically either store the recorded images and video for later retrieval or they transmit them to the remote process or person employing the Screen Scraper. There are some legitimate uses of screen scrapers, but they are often used maliciously by attackers to surreptitiously track behavior to perform unwanted or unauthorized actions that can include identity theft.

Security Analysis Software: Any program used by a computer user to analyze or circumvent security protections.

Snoopware: Sometimes used as a synonym for the narrower definition of Spyware—i.e. *Tracking Software*.

State Management Tools: Technologies used to store and make available information about the "state" of a system—i.e. information about current conditions and operations. Cookies are the most common form of a State Management Tool since they can be used to store data provided to a Web site and maintain a Web application session. State Management Tools can be used as a *Tracking Technology*.

System Modifying Software: Any program used to modify a user's system and change their experience, such as by altering their home page, search page, default media player, or lower level system functions.

Spyware: The term Spyware has been used in two ways**.**

In its narrow sense, Spyware is a term for *Tracking Software* deployed without adequate notice, consent, or control for the user.

In its broader sense, Spyware is used as a synonym for what the ASC calls "Spyware and Other Potentially Unwanted Technologies."

In technical settings, ASC uses the term Spyware only in its narrower sense and always marks it as such [spyware(narrow)]. However, we understand that it is impossible to avoid the broader connotations of the term in colloquial or popular usage, and we do not attempt to do so. For example, we refer to the group as the Anti-Spyware Coalition and vendors as makers of anti-spyware software, even recognizing that their scope of concern extends beyond tracking software. Therefore, the term spyware, when used generally in an ASC document will always refer to the broader colloquial usage.

Stream Files: See "Alternate Data Stream."

System Monitor: *Tracking Software* is used to monitor computer activity. System Montiors range in capabilities but may record some or all of the following: keystrokes, screen captures, e-mails, chat room conversations, instant messages, Web sites visited, programs run, time spent on Web sites or using programs, or usernames, passwords or other types of data in transit. The information is typically

either stored for later retrieval or transmitted to the remote process or person employing the Monitor. Keyloggers and Screen Scrapers are types of System Monitors.

Tracking Cookies: A Tracking Cookie is any cookie used for tracking users' surfing habits. Tracking Cookies are a form of *Tracking Technology*. They are typically used by advertisers wishing to analyze and manage advertising data, but they may be used to profile and track user activity more closely. However, tracking cookies are simply a text file, and far more limited in capability than executable software installed on users' computers. While installed software can potentially record any data or activity on a computer (see *System Monitor*), cookies are simply a record of visits or activity with a single Website or its affiliated sites.

Tracking software: Software that monitors user behavior, or gathers information about the user, sometimes including personally identifiable or other sensitive information, through an executable program.

Tricklers: *Automatic Download Software* designed to install or reinstall software by downloading slowly in the background so the download is less noticeable (and does not impair other functions). Tricklers are typically used to enable a spyware program to install silently or to reinstall after a user has removed components of the program from his or her computer.

Trojan: A Program that appears to do one thing but actually does another (a.k.a. Trojan Horse).

Underlying Technology: One of the technologies listed in the table above that has been used to harm users; however with proper notice, consent, and control, these same technologies could provide user benefit.

United Virtualities Persistent Identification Element (PIE): United Virtualities PIE is a *Tracking Technology* designed to be an alternative to a cookie, utilizing Macromedia Flash, that is an example of a passive tracking technology.

User: The system owner or their designated administrator. In a household, this is commonly the person operating the computer.

Virus: A computer virus is code that recursively replicates a possibly evolved copy of itself. Viruses infect a host file or system area, or they simply modify a reference to such objects to take control and then multiply again to form new generations.

Worm: Worms are network viruses, primarily replicating on networks. Usually a worm will execute itself automatically on a remote machine without any extra help from a user. However, there are worms, such as mass-mailer worms, that will not always automatically execute themselves without the help of a user.

Zombie: A system that has been taken over using *Remote Control Software.* Zombies are often used to send spam or to attack remote servers with an overwhelming amount of traffic (a Distributed Denial of Service Attack). A collection of many zombies comprise a botnet.

Vendor Dispute and False Positive Resolution Process

Anti-Spyware vendors are often approached by software publishers alleging that their programs have been unfairly flagged as "spyware." This document provides an overview of generally accepted practices for processing and resolving such disputes. The document is meant as a common, transparent set of best practices that anti-spyware vendor practices may exceed. To be clear: vendor dispute processes are run by individual anti-spyware companies or software publishers. The Anti-Spyware Coalition neither runs such a process independently nor acts as a party in them.

Publisher Disputes/False Positive Claims

1. Process Overview

a. Submission

- A software publisher may wish to initiate a review if it believes that a program or associated files have been incorrectly classified by a particular anti-spyware vendor, or it has recently updated the behavior of its program and believes it should no longer be classified as spyware.
- To initiate the review, the software publisher visits the Web site for the anti-spyware vendor and submits a designated form. Alternatively, if the anti-spyware publisher does not have a Web form, the software publisher can send an email or postal inquiry to a designated email or postal address.
- The Software publisher must supply all required information in order to request review by the anti-spyware vendor.
- The anti-spyware vendor will acknowledge receipt of the disputing publisher's request.

  Note: Anti-spyware vendors may handle queries submitted by third parties and end users (not the software publisher) using a separate process or channel.
- During the dispute resolution process, the anti-spyware vendor may request additional information such as:
  - A copy of the current version or versions of the software;
  - Information about all substantial means by which the software is distributed, potentially including specific information about one or more affiliates or distributors;
  - A listing of specific distribution requirements placed on affiliates or distributors, ways in which the requirements are enforced, and any known deviations from them;
  - Known ways in which the behavior of any submitted software can be changed from its default behavior;
  - Ways in which any submitted versions differ from other versions including descriptions of how the behavior of the software has changed and how the underlying files can be distinguished;
  - The version of the anti-spyware software and signature file that the dispute concerns;

- Any additional information the anti-spyware vendor believes is relevant to its analysis.

This information will typically be requested either as part of the publisher dispute form or in a follow-up e-mail. In order for the review to continue, the software publisher must respond to these queries.

- If a disputing publisher fails to provide required information to the anti-spyware vendor, the case may be closed by the anti-spyware vendor. If a case is closed the software publisher must resubmit a vendor dispute form or send a new email (including all required information) to activate a new dispute.
- The anti-spyware vendor may decide to have the entire dispute resolution process handled by an independent third-party chosen by the vendor.

b. Analysis and Response: The anti-spyware vendor will acknowledge, in writing, upon receipt of the complaint and start the dispute resolution process.

- The anti-spyware vendor will attempt to fairly and accurately recreate the user experience and compare the behavior of the product against the anti-spyware vendor's current analysis criteria. Data collection for researching an application includes screen shots, video captures, log files, characteristics of the application analyzed, the signature criteria, and the detection technology.
- If the application meets the anti-spyware vendor's criteria for detection, detection may persist. The software publisher will be notified at this point in writing with a general indication of the criteria that were matched.
- If the application does not meet a sufficient amount of criteria, the anti-spyware vendor may choose to remove detection of the software from the signature library or change the way the product is described. The software publisher will be notified in writing of the results in a timely manner. The notice will include information on a timeframe to implement the decision. Other versions of the same software may continue to be detected so long as they still meet a sufficient amount of the anti-spyware vendor's criteria for detection. In the case of a clear false positive, the anti-spyware vendor may contact the software vendor via e-mail to confirm the issue and discuss next steps for resolution.
- The anti-spyware vendor will respond to all complaints within a reasonable timeframe. Response time is dependant on several factors including, but not limited to:
  - The potential impact on users of ceasing detection
  - The technical demands of analysis
  - The completeness of the information provided
  - The complexity of a particular case.
- In communicating the dispute decision to the disputing software publisher, the anti-spyware vendor will state to the software publisher that decisions are subject to change if alterations are made to the program over time or as classification criteria and/or detection technology employed by the anti-spyware program changes over time to address the evolving landscape.

c. Resubmission

- A software publisher may choose to resubmit its program for reconsideration if it has implemented updates that change a program behavior sufficiently that it reasonably believes address the anti-spyware publisher's concerns.
- Anti-spyware vendors may establish limits to the number of times a program is submitted for review. These requirements can be time-bound by a reasonable waiting period and/or activity bound (e.g. only when the software vendor's program changes).
- In general, it is not the responsibility of anti-spyware vendors to enter into ongoing relationships with adware makers or other software publishers in order to assist them in revising their software and business practices. Anti-spyware vendors may choose to give advice, but should not be expected to serve as free consultants, to police software distribution networks, or to provide a general vetting service for software development.

2. Suggested best practices

- **Publishing overview of criteria**: Anti-spyware vendors should publish an overview of their analysis approach and criteria to give software publishers and users a better understanding of how programs will be reviewed. It is not necessary, however, to disclose detail or point-by-point review analysis.
- **Published process for resolving disputes:** Anti-spyware vendors should publish their process for resolving disputed detections. This should include how a software publisher can submit a dispute and what it can expect throughout the process and the policy on resubmission.
- **Electronic submission of vendor disputes:** Anti-spyware vendors should provide an easy means for software publishers to contest detection/classification in the signature library. A publisher dispute form provides software publishers with an understanding of how to get the process started. It should be available through the Internet and should clearly indicate the information needed from the software publisher to start the analysis.
- **Documented publisher dispute process:** Anti-spyware vendors should keep appropriate records of publisher disputes received, as well as documentation for the analysis conducted and support for the conclusion. The anti-spyware vendor should provide appropriate documentation on its conclusions to the software publisher.
- **Communications in writing:** Communications between the software publisher and the anti-spyware vendor should generally be in writing. This provides a documented record of interactions and reduces the potential for misunderstandings.
- **Setting expectations:** Regardless of whether the review was in favor of the software publisher or not, the anti-spyware vendor should highlight to the software publisher that decisions are subject to change if alterations are made to the disputed programs over time or as the signature criteria and/or detection technology employed by the anti-spyware program changes over time to address the evolving landscape. However, see note above about the reasonable expectations of the role of anti-spyware companies in ongoing review.

Working Report October 27, 2005

Safety Tips for Fighting Spyware

The best defense against spyware and other unwanted technologies is to prevent them from getting on your computer in the first place. Awareness is the best approach to protect yourself online, so staying up-to-date on current threats and safe surfing practices is essential. Here are some steps you can take to stay safe while still getting the most from the Internet and software programs.

Keep security on your computer up to date.

- **Update security patches:**
  Many malicious spyware developers exploit known security holes in essential software, such as operating systems and browsers. Update essential software frequently. Automate the process if your vendor offers the option.
- **Security and privacy settings in Internet browsers:**
  Many Internet browsers have security and privacy settings that you can adjust to determine how much—or how little—information you are willing to accept from a Web site. Check the documentation or help file on your Internet browser to determine how to adjust these settings to appropriate levels. See GetNetWise.org for detailed instructions:
  http://privacy.getnetwise.org/browsing.

Download programs only from Web sites you trust.

- If you are not sure whether to trust a program you are considering downloading, ask a knowledgeable friend or enter the name of the program into your favorite search engine to see if anyone else has reported that it contains spyware or other potentially unwanted technologies.
- Look carefully at the address of the site you are visiting to make sure it is not an obvious spoof.
- Be particularly suspicious of programs you see advertised on unrelated Web sites. If a maker of a screensaver, "smiley" inserter, or other program heavily promotes its purportedly-free product, the product may include extra software you do not want.

Beware the fine print: Read all security warnings, license agreements, privacy statements, and "opt-in" notices with any software you download.

- Whenever you install something on your computer, make sure you carefully read all disclosures, including the license agreement and privacy statement. Sometimes important information such as aggressive installs or the inclusion of unwanted software in a given software installation is documented, but it may be found only in the EULA. The fine print may be the only place consumers can find notice of potentially unwanted technologies. Unfortunately, careful consumers must read *all* the fine print.
- When given the choice of opting into something, make sure you understand fully to what you are agreeing.
- If you have doubts about the legitimacy of the software, do not install it, or go to a trusted source to find more information about the software. To be safe, you should never install software if you are uncertain about it.

Don't be tricked into clicking: You don't have to click "OK," "Agree," or "Cancel" to close a window.

- If you want to close a window or dialog box, consider the options provided by your operating system or Web browser, such as closing the window with the 'x' mark in the upper corner or typing Alt+F4 in Microsoft Windows.
- Pay attention when closing windows; some dialog boxes may have a prominent statement that says, "Click here to close window," then in less prominent text adds, "and install software."

Be especially careful with certain types of "free" programs.

- Many file sharing applications are bundled with other, potentially unwanted software.
- Similarly, screen savers, cursor enhancements, wallpaper bundles, "smiley" inserters and any other software promoted aggressively often include extra software you did not request and aren't expecting. Be sure you clearly understand all of the software packaged with those programs.

Use available tools to detect and delete spyware.

- There are a number of security tools available from a variety of vendors that can help you identify spyware, stop the installation of it on your PC, and/or remove it.
  - **Anti-spyware and Anti-virus software:**
    There are a number of programs (available both free and for a fee) from reputable vendors that can help detect spyware, prevent spyware from being installed on your PC, and/or remove spyware if it is installed. (Some programs can be removed through "Add/Remove programs" or other standard operating system features.) Note that some software that claims to be an anti-spyware tool is actually adware or other potentially unwanted software in disguise. For this reason, you should read reviews to be sure any anti-spyware software you download is from a reputable publisher.
  - **Personal firewall:**
    Installing and using a firewall provides a helpful defense against remote installation of spyware by hackers.

We encourage you to learn more about how to protect yourself from spyware by visiting the US federal government OnGuard OnLine Web site at http://www.onguardonline.gov.