Anti-Spyware Coalition
Definitions and Supporting Documents

Spyware is increasingly becoming one of the Internet's most prevalent threats. Computer users are looking for ways to regain control over their own computers. Many find themselves in a constant battle against programs that sneak onto their computers, track their online activities, open security holes, impair the performance and stability of their systems, disrupt their computer use with unwanted advertising, or frustrate their attempts to remove or disable these behaviors. These programs find their way onto computers through deceptive installations and bundling arrangements with unmanaged third-party distributors, by exploiting security holes, through social engineering and through diverse other means.

In the face of this threat, the technology industry has provided technical solutions and together with consumer advocates produced educational materials for consumers. Anti-spyware companies offer software to alert consumers about spyware and other potentially unwanted technologies, and to help block or remove them. These companies exercise their critical judgment to give consumers guidance about what software they may want and what software they might wish to avoid. By providing this service, the companies offering anti-spyware software strive to advance transparency and user control.

However, to further help consumers protect their privacy and security, the anti-spyware industry will benefit greatly from clear, agreed-upon language for describing these threats. Such language will enhance and clarify the communication between technology companies and their customers as well as with policy makers, third-party software vendors, and others.

The attached documents aim to advance this definitional purpose.

- *Spyware and Other Potentially Unwanted Technologies* defines the user concern that anti-spyware vendors seek to address and provides examples of such potentially unwanted technologies.

- The *Glossary* defines terms commonly used in discussions about spyware and other potentially unwanted technologies.

- *Vendor Dispute Resolution Process* details the process a software publisher can expect an anti-spyware company to follow if the publisher feels that its software has been inappropriately described or categorized.

- In addition, we have developed *Anti-Spyware Safety Tips* to provide some basic tips for consumers to protect themselves and their computers.

The Anti-Spyware Coalition views these documents as the first step in an ongoing process to address a range of issues. While these documents do not create objective criteria, best practices, or risk modeling procedures, we hope to begin to address these issues using these documents as a starting point. We look forward to feedback from all interested parties.

The Center for Democracy and Technology convened 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 implemented in ways that impair users' 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
- Collection, use, and distribution of their personal or otherwise sensitive information

These are items that users will want to be informed about, and which the user, with appropriate authority from the owner of the system, should be able to easily remove or disable.

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.

Common Terms for 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 • Keylogger • 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 cause personal information to be shared widely or allow it to be stolen, resulting in fraud or ID theft. • Can slow machine down • May be associated with security risks	• 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	Used to display advertising content (e.g. pop-ups)	• May be a nuisance and impair productivity • May display objectionable content • Can slow machine down or cause crashes and loss of data • 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.
• Backdoors • Botnets • Zombie • 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 • Done covertly, it is stealing cycles and other resources • Can slow machines down.	• 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	• May be used for desirable customization
• Hacker Tools	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

Examples of Spyware and Potentially Unwanted Technologies (continued)

Common Terms for Unwanted Varieties	Underlying Technology	Description of Underlying Technology	Why the Underlying Technology May Be Unwanted	Why the Underlying Technology May Be Wanted
• 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
• Tracking Cookies and other similar technologies (e.g. PIE)	Other Tracking Technologies	Used to gather limited information about user activities without installing any software on the user's computers	• May allow unwanted information to be collected about visited web sites	• May be used for desired customization or personalization : e.g. "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

ActiveX Control: See “Browser Plug-in.”

Adware: A type of *Advertising Display Software*, specifically certain executable applications whose primary purpose is to deliver advertising content in a manner or context that potentially may be unexpected and unwanted by users. Many Adware applications also perform tracking functions, and therefore may also be categorized as *Tracking Technologies*. 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. 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.

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 anti-virus and backup tools do not process these streams, so they are sometimes used to hide spyware and other potentially unwanted software.

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 cracked machines running programs (worms, trojans, etc.) under a common command and control infrastructure. Botnets have been used for sending spam remotely, installing more spyware without consent, and other illicit purposes.

Browser Help 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 can offer searching or anti-phishing services. Plug-ins can also be used to perform potentially unwanted behaviors such as redirecting search results or monitoring user browsing behavior, 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 Internet Explorer web browser.
> **Browser Helper Object (BHOs):** A Type of Browser Plug-in that is executed each time the Internet Explorer web browser is launched. Toolbars are a common form of BHO.
> **Firefox Extensions:** A type of Browser Plug-in that is executed each time the Firefox web browser is launched. Extensions can add anything from a toolbar button to a completely new feature.

Bundling: The practice of distributing multiple pieces of software together, so that when the software “bundle” is installed, all components are installed. In many cases, bundling is a convenient way to distribute many related pieces of software together. However, in some cases, unwanted software components can be bundled with programs users download, and can thereby be snuck onto their computers without adequate notice or consent.

Cookie: A piece of data that a web site, through the means of the browser, saves on users' computers' hard drives and retrieves when they revisit that Web site or an affiliated 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 you have visited, etc.

Dialer: A program that utilizes a computer's modem to make calls or access services. Users may want to remove dialers that can result in unexpected phone numbers being dialed or unexpected telephone charges. Dialer is a colloquial term for *Dialing Software*.

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 typically launched using the compromised systems of Internet users. 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 communicate with other systems 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 systems, browsers, anti-virus applications and anti-spyware tools. 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: Software that is automatically downloaded to a user's computer when she visits a website 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 a security hole 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 or to 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 parameters of use granted to the user. The software producer specifies these parameters and limitations on use, which can become part of a legally binding contract. Some companies use the EULA as the sole means of disclosure of a program's behaviors or bundling.

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.
Flash: (see Macromedia Flash)

Hacker Tool: *Security Analysis Software* that can be used to 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.

Keylogger (or Keystroke Logger): *Tracking Software* that surreptitiously 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.

Macromedia Flash: A platform that supports the authoring and display of multimedia content (e.g., graphics, audio, and/or streaming media). Flash content can appear in a web page or be stored in file. Playing Flash content within a browser is typically done through a Browser Plug-in that includes the Flash player. The Flash player is pre-installed in several web browsers and on different operating

systems. Flash MX technology includes a mechanism that can be used as alternative to tracking cookies (see PIE).

Password Cracker: *Security Analysis Software* designed to allow their users to recover or decrypt lost, forgotten or unknown passwords. While a legitimate tool used by security administrators and law enforcement officers, Password Crackers pose a significant security and privacy threat when used illicitly by unauthorized users.

Persistent Identification Element (PIE): PIE is a *Tracking Technology* designed to be an alternative to a cookie that uses Macromedia Flash local shared objects to identify visitors.

Port Scanner: *Security Analysis Software* used to discover what computer network services a remote system provides. Port scanning gives an assailant an idea 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.

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 that do not pose security threats, they can be used maliciously by attackers to start or end programs, install and uninstall new software, or perform other potentially unwanted or unauthorized actions.

Rootkit: A set of programs used to hack into a system and gain administrative-level access. 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. Rootkits are an extreme form of *System Modification Software*.

Screen Scrapers: *Tracking Software* that surreptitiously 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.

Snoopware: Sometimes used as a synonym for the narrower definition of Spyware—i.e. *Tracking Software* deployed without adequate notice, consent, or control for the user.

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 State Management Tool. State Management Tools can be used as a *Tracking Technology*.

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, we use the term Spyware only in its narrower sense. 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.

Stream Files: See "Alternate Data Stream."

System Monitor: *Tracking Software* used to monitor computer activity. System Montiors range in capabilities but may record some or all of the following: keystrokes, e-mails, chat room conversations, instant messages, Web sites visited, programs run, time spent on Web sites or using programs, or usernames and passwords. 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 far more limited in their ability to track users than software that is actually installed on users' computers. While installed software can potentially record any data or activity on a computer (*see* System Monitor), cookies can only record visits or activity on a single website or its affiliated sites. Moreover, unlike Tracking Software, cookies entail no substantial effect on computer reliability, security, or speed.

Tricklers: *Automatic Download Software* designed to covertly install or reinstall software by downloading slowly in the background so the download is less noticeable. 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 non-replicating malicious program designed to appear harmless or even useful to the user, but, when executed, harms the user's system. Some software bundles containing malicious forms of spyware or other potentially unwanted software are considered to be Trojans.

Virus: Self-replicating code that propagates by reproducing and inserting itself into other programs, documents, or email attachments. Some viruses are intentionally destructive (for example, erasing information on users' hard drives). For others, the primary negative effect is their uncontrolled self-reproduction, which can overwhelm system resources.

Worm: A computer worm is a self-replicating computer program, similar to a computer virus. Unlike viruses, however, worms self-propagate and so do not require other programs or documents to spread. Worms typically spread through email or other file transmission capabilities found on networked computers.

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).

Vendor Dispute and False Positive Resolution Process

This document provides an overview of generally accepted practices relating to the processing of publisher disputes and alleged false positives by anti-spyware vendors. It is meant to provide guidance to software publishers and community advice for anti-spyware vendors. The document is meant as a common, transparent set of best practices which 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 in the signature library of 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.

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

- The anti-spyware vendor will attempt to 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.
- 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 (e.g. every 90 days) 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.
- **Electronic submission of vendor disputes:** Anti-spyware vendors should provide an easy means for software vendors 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.
- **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.

Anti-Spyware Safety Tips

The best defense against spyware and other unwanted technologies is to prevent them from getting on your computer in the first place. Here are some steps you can take to stay safe while using 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 vender 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

Only download programs 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 a spoof.
- Be particularly suspicious of programs you see advertised on unrelated web sites. If a maker of a screensaver, “smiley” inserter, or other program resorts to banner ads to promote its purportedly-free product, the product may include extra software you do not want and did not expect.

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 (both free and for 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.