

Anti-Spyware Coalition Definitions Document

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 uninstalled. 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 technologies. 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 technologies and help consumers better understand how those tools work to defend them. The following documents represent the completion of the 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.

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. An underlying technology typically becomes unwanted when it is implemented in a way that provides no benefit to -- or actively harms -- authorized users.

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