BEFORE THE FEDERAL TRADE COMMISSION

SPYWARE WORKSHOP – COMMENT, P044509

Submitted by: AWS Convergence Technologies, Inc. & WeatherBug.com

I. Introduction

AWS Convergence Technologies, Inc. ("AWS") is the developer of the popular desktop software application WeatherBug®. AWS is submitting this comment pursuant to the Commission's Federal Register Notice of February 24, 2004.

AWS owns and operates the world's largest live weather network. With more than 7,000 weather-monitoring stations nationwide, the WeatherBug Network is the most granular network available, with monitoring stations located primarily at schools across the country.

AWS developed the underlying technology for this weather network, and currently applies the network into the following areas:

Broadcasting. AWS partners with about 100 NBC, ABC, CBS and Fox televisions stations to stream live data from our network into the weather segment of their newscasts. A few examples: our partner in Washington DC is WRC (NBC4), our partner in New York is WNBC, and our partner in San Francisco is KPIX (CBS 5)

Education. We provide each of our 7,000 school clients with "WeatherBug Achieve," a K-12 curriculum that utilizes the data collected by our weather tracking stations to teach about science and math. AWS's CEO, Bob Marshall, serves as chairman of the Maryland State Education Technology committee, which reports to the state superintendent. Marshall was the 2003 NASBE (National Association of State Boards of Education) Award winner for contributions to education. In 2001 he was awarded the ComputerWorld Smithsonian Laureate award for co-founding and developing AWS' school WeatherNet program. The WeatherBug Achieve (formerly WeatherNet Classroom) educational curriculum was also honored as the Education Technology of the Year by Media and Methods magazine (an education publication).

Industry. AWS Data Services provides data from its network to more than twenty major energy providers, such as Constellation, Entergy, AEP and others to help them better forecast energy load, and manage supply.

Government. In its partnership with the National Weather Service and NOAA, AWS has agreed to provide live weather information to the government and emergency planners in cases of threats to life or property. This partnership was arranged shortly after 9/11, chiefly because the WeatherBug network is the only nationwide source capable of tracking hyper-local weather conditions in real-time. In addition, according to the National Weather Service per a discussion in 2002, WeatherBug is the number one distributor of National Weather Service warnings and alerts.

Consumers. In Spring of 2000, AWS launched the desktop application known as WeatherBug. This sponsor-supported product gave consumers direct access to our national network for the first time, at no charge. WeatherBug was originally launched as a new component of our service to our broadcast television partners. Today, most of our television partners distribute a localized version of WeatherBug to their viewers. They promote it on-air during newscasts and also through television promotional announcements and via their website. As such, WeatherBug has emerged as a well-known national brand. AWS also promotes WeatherBug online for free download at weatherbug.com. To date more than 32 million consumers have downloaded WeatherBug, and more than thirty-thousand new registrants sign-up for WeatherBug every day, making it one of the most popular Internet services in the United States.

AWS is committed to the fight against Spyware. As a leading application developer, AWS is acutely aware of both the power of desktop applications, and the responsibility to design, deploy and manage them with integrity. Applications that are tailored to a specific task (such as Outlook for email, or WeatherBug for real-time weather conditions) allow users to harness the Internet in ways impossible for static web sites. A prime example of this is the wide-spread, timely distribution of National Weather Service warnings delivered by WeatherBug. As a desktop application, WeatherBug is able to proactively warn users of impending severe weather, as opposed to the reactive nature of web site updates. However, we also constantly recognize that we have been invited onto the desktop. We realize that we will be allowed to remain only as long as we respect the rights and wishes of our users.

Since its inception, AWS has been a leader in shaping best practices, and providing the consumer with notice and control – true choice – in their experience and interaction with our products. As such, we welcome the opportunity to submit these comments and to help frame the policy debate on Spyware. It is vitally important that all responses to the Spyware problem – legislative, regulatory and industrial – are coordinated, measured and nuanced so as to counter only the bad actors. Casting too wide a net threatens to chill software innovation, disable legitimate revenue and distribution models, and limit valuable consumer services. AWS agrees with those that advocate regulating behavior, i.e., the use of technology, rather than regulating technology itself.

II. Defining and Understanding Spyware

Many have commented on the difficulty in defining Spyware. Over the last several years many widely disparate definitions have been proposed, encompassing everything from the truly malicious to the merely annoying. While some definitions have focused on the capability present in a piece of software, i.e., technology, AWS believes that the better definitions focus on the uses to which the software is put, i.e. behavior. Moreover, because the label “Spyware” itself is so pejorative, one must be careful not to so brand legitimate technology through sweeping generalizations about its capability. “Spying” implies deception, deceit, and stealth; in other words it implies particular inappropriate behavior.

AWS subscribes to the definition put forth by, among others, the DCIA in its Comment of March 19, 2004, to wit:

> "The DCIA broadly defines 'spyware' as software installed without consent that provides no benefit and, more specifically, as a pejorative term to describe software that installs itself on consumers' personal computers without their knowledge or consent and does one or more of the following: gathers personal data about users and/or tracks their usage behavior without consent, supplies this information to undisclosed third parties for undeclared purposes, utilizes processing capabilities for unknown tasks without permission, and makes itself difficult to uninstall."

AWS believes this definition to be particularly apt, as it focuses on the improper, invisible, and nefarious behavior indicative of true Spyware.

Spyware vs. Adware

The Commission has asked how Adware is different, if at all, from Spyware. AWS defines Adware as software whose sole functionality is to display advertising. Examples of Adware include WhenU's SaveNow! and Claria's GAIN. AWS believes that there is nothing inherently objectionable about Adware ***provided*** that the software installation and operation is preceded by meaningful notice and consent. Meaningful, in this context, means that the providers of these products must clearly and completely disclose the value proposition and functionality of the software ***before*** installation, provide adequate disclosures during operation, and allow appropriate user choice and control over removal. If such is the case, consumers have been enabled to make an informed choice.

An important distinction should be drawn, however, between Adware (as defined above) and "advertising-supported software." Unlike Adware, whose sole functionality is to display advertisements, advertising-supported software presents a core value proposition and functionality that is of benefit to the consumer, and separate and apart from its ability to serve advertisements. The CDT, in its Comment of March 4, 2004, highlighted the Eudora email application as a "…successful and user-friendly example of ad-supported software." Advertising support is a legitimate revenue model that allows software developers a means to offer beneficial software at little or no cost to consumers. Other examples of successful ad-supported software products include AOL Instant Messenger, eFax, The Weather Channel's Desktop Weather, and WeatherBug.

III. Distribution of Spyware

AWS has no particular knowledge regarding the distribution methods employed by Spyware merchants. However, the literature is replete with stories regarding common tactics. Two of the more pernicious methods are the so called "drive-by download" and the "back door" installation. Generally speaking, a "drive-by download" occurs without any notice whatsoever to the user, as the result of doing something as innocuous as opening a web page. There is no indication that a download has begun or is occurring. Similarly, a "back door" installation exploits security holes in the web browser or operating system of a user's computer, to effect the installation of software without knowledge or consent. Clearly these behaviors are reprehensible, and have no legitimate place in commerce.

A third method mentioned frequently in the literature is the concept of “bundling.” Bundling is the practice of combining two or more software applications into a single installer file, so that all are downloaded and installed together. Bundling is not inherently a bad or improper practice. In fact, it is a common marketing method in both online and traditional commerce. When deployed appropriately, and accompanied by adequate disclosures and consent opportunities, bundling can be a very cost-effective method for software distribution. Therein, however, lies the rub – Spyware merchants have exploited the bundling concept to sneak their programs onto computers, without notice or consent, in the slipstream of other benign programs that have a discrete and reasonable value proposition.

It should be noted that download distribution is an extremely popular, efficient, and economical software distribution method. It provides economies that could never be reached if software distribution were confined to boxed, shrink-wrapped methods. A glimpse at CNet’s Download.com page shows that its 25 most popular programs for the week ending May 10, 2004 were downloaded 7,055,350 times in that week. These same 25 programs have been downloaded from that site a total of 1,224,734,244 times. The proliferation of Spyware threatens the existence of this extremely popular and economic model. It is vitally important that industry, legislative and regulatory responses to Spyware be structured in a way so as to protect consumers’ faith in download distribution, not degrade it through overly broad or poorly defined approaches.

IV. Effects of Spyware

The effects of Spyware to individual users are well documented. AWS has no particular expertise in this area, although we have gained insight into the problem through our interaction and communication with our user base. Our technical support team answers hundreds of emails every day, in which WeatherBug users ask for help regarding technical problems, largely as a result of having myriad applications on their computer desktop**.** Accordingly, our staff has become adept at guiding a user through his or her system in an effort to find the malicious or inefficient code that is causing the problem.

It appears that the major Spyware effects can be grouped into three broad categories:

- **Privacy concerns/Identity theft –** primarily the result of pernicious use of key loggers and other true “spying” conduct
- **Computer Security** – akin to the above, but primarily the result of software exploiting security holes and leaving such holes open for others, such as hackers, etc.
- **Economic Loss –** this takes many forms, such as hidden “dialer” programs, resource hogging, system crashes, etc.

An additional effect, alluded to above, is an increase in “Download Anxiety,” or consumer fear and uncertainty regarding the relative safety of downloading software. Such consumer uncertainty threatens economic harm to the software industry as a whole.

A well-meaning but often frenzied press, imprecisely drafted legislation, and industry silence only compound this problem.

V. Responses to Spyware

As was made very apparent by the panelists and contributors to the Commission's April 2004 workshop, formulating a strategy for combating Spyware poses a number of challenges. Despite such challenges, AWS believes that measured responses should be employed. Most of the more insidious practices of the Spyware merchants are already illegal under a number of federal statutes, including Title 5 of the FTC Act, the Computer Fraud and Abuse Act, and others. Vigilant law enforcement against the illegal behavior identified through this workshop will go a long way to putting a lid on Spyware proliferation. The current state and federal bills now pending, which have the Spyware problem as their chief focus, are laudable, well intentioned efforts to stop the spread of Spyware. Unfortunately, many of these bills suffer from the same problems that have plagued industry – incomplete information and shifting, imprecise definitions. Some of these bills are over-inclusive, some are under-inclusive, and some are paradoxically both.

That being said, AWS believes that there is a place for well-constructed federal legislation addressing this problem. Such legislation should focus on improper behavior, much as the CAN-SPAM Act and the Computer Fraud and Abuse Act do. These laws focus on the misuse of technology, not the underlying technology itself. In addition, a federal law, if structured to pre-empt state laws, will ease the burden on the software industry that would otherwise be posed by fifty separate state approaches. AWS intends to reach out to Congress, in an attempt to help frame the policy debate in that forum.

AWS believes, however, that new legislation (and the enforcement of existing legislation) is not the complete answer. What is necessary is a coordinated campaign by industry to create best practices and inform the public (and media) where the line is drawn between good and bad actors. As stated above, efforts to throw a net around specific technological capability employ a false logic. Industry – developers, security professionals, technologists, trade groups – must all mount a coordinated campaign to establish a code of conduct, and communicate it clearly to all constituents.

To be effective, this code of conduct must reflect the hallmarks of Consumer Choice. For choice to be meaningful in any situation, it must be predicated upon adequate information, and acceptable alternatives must be available. AWS believes that Consumer Choice, in this arena, is built on three principles:

- **Meaningful Notice** – clear, concise language disclosing software author, functionality, information collection practices, advertising practices, and communication architecture. It must be devoid of legalese, obfuscation and circular references.
- **Informed Consent** – a close cousin to Notice, proper consent practices should offer a user choice any time there are optional features, or privacy-sensitive functionality. The optional functionality within the Google Toolbar, which allows a user to accept or decline PageRank monitoring, is a prime example of a best practice in this regard.

- **User Control –** consumers should be allowed to change their minds. They should have an unfettered right to remove software, and the uninstall protocol should be accomplished easily, rapidly and with no complications.

An emerging best practice is what AWS calls "on-going opt-in." This is a practice of regularly touching consumers with disclosures and consent opportunities. We believe that it helps foster trust, and cements user loyalty.

In addition to best practices, industry should agree upon a mechanism for validation. This can take many forms, for example, a "Seal of Approval" from a trusted third party, a "User's Bill of Rights" widely adopted, and so on. This effort will require cooperation among industry, government and public interest groups to insure an appropriate validation platform – a necessary launch-pad to effective consumer education.

V. Conclusion

AWS has long been an advocate of user privacy protection and a steadfast advocate against Spyware. We have joined with other like-minded companies and organizations in the fight against Spyware, as a member of TRUSTe, and as an early member of the Consortium of Anti-Spyware Technology (COAST) - a non-profit organization that has been established to create a forum where members can collaborate on a wide range of projects designed to increase awareness of the growing Spyware problem facing everyone using the Internet.

AWS is working with the other members of TRUSTe and COAST to help establish anti-Spyware standards for software and to help consumers make more informed decisions about the Internet-enabled software they place on their computer.

In addition, AWS offers links to popular anti-spyware applications on weatherbug.com. While AWS does not endorse any specific Spyware detection products, we encourage our users to download popular Spyware detection software directly from our website for their protection. The developers of these products advertise them as reliable and effective programs in controlling and detecting Spyware.

In closing, AWS applauds the Commission's efforts in focusing discussion on this serious problem. We look forward to a continuing constructive dialogue on these issues, and to working with all interested parties towards a thoughtful resolution.

Respectfully submitted,

Daniel W. O'Connell
General Counsel and CPO
AWS Convergence Technologies, Inc
2-5 Metropolitan Court
Gaithersburg, MD 20878
301-258-8390 ext. 138
doconnell@aws.com
http://www.aws.com