

October 27, 2005

**Anti-Spyware Coalition Summary
of comments and ASC response on the
July 11, 2005 Public Comment Draft of the
*ASC Definitions and Supporting Documents***

Summary

In the four weeks since the Anti-Spyware Coalition (ASC) released the public draft of its *Definitions and Supporting Documents*, ASC received almost 400 comments.

As we document in this report, ASC also made many changes based on specific issues raised in the comments. We are grateful to the hundreds of individuals, organizations and companies that engaged in this process.

ASC did not view the comments as a vote or a popularity contest. We were strictly interested in substantive comments. However, it is important to that an almost equal number of comments were concerned that the definitions were too vague (and therefore not as helpful as they could be to software companies trying to do the right thing) as those who thought they were too specific (and therefore too helpful to spyware companies). In general, ASC was reassured by the comments that the documents were useful to moving forward in a process to help anti-spyware companies communicate better amongst themselves and with consumers.

Many of the comments implied or directly suggested that it was difficult to comment on definition without the specific objective criteria standards, risk modeling or best practices for which they will be used. As a result, ASC felt that it was important to stress that the definitions are a living document. As such, we have called this version the “Working Report” to show that it is open to changes as we develop the other documents and beyond. We hope that we can continue to engage a wide range of players in the future and hope to utilize academic and otherwise independent research in this process.

ASC definitions comments

These comments can be roughly divided into thirteen different categories:

- Positive feedback with no substantial comments on the document itself
- Comments raising concerns about the role of user consent and the use of End User License Agreements (EULAs)
- Apprehension about the creation of a solid definition
- Viewpoints on the main definition of spyware
- Negative comments about the coalition or specific companies involved
- Comments expressing confusion about the precise purpose of the documents
- Comments primarily concerned with recognition and deletion of potentially unwanted programs

October 27, 2005

- Comments expressing interest in a risk modeling document
- Comments concerned that the definitions may be too broad or too narrow
- Comments specifically on the Vendor Dispute document
- Specific line item or vocabulary edits.
- Substantial comments that fall under more than one of the above categories
- Miscellaneous comments

Many comments were ambiguous or contain comments that fit within two or more of these categories. However, comments have been placed in the category in which the most detailed comments and suggestions belong.

Positive Feedback

ASC received a large number of very general kudos that required no real response from the Coalition. These comments came from a range of individuals from many different fields, companies, and nations. The kind of positive response the Coalition has received as a result of the initial release of these documents is a significant indication that this effort has been long awaited and will mark a significant step in the battle against spyware.

Consent and EULA concerns

A significant number of comments address people's concern about their ability to control the programs that are installed on their computers. These comments urge the coalition to address:

- What constitutes adequate notice and consent
- The types of questionable EULA practices in which companies who produce adware and spyware engage.
- How much responsibility a user has to read and understand the entirety of a long EULA.

The question of how to deal with EULA's that are deliberately deceptive or overly complicated is clearly central to the issues involve. This question will continue to be central to the Coalition's EULA's are central to the presence of notice, consent, and control and while standards are not present in these Documents, future coalition releases will address these issues. As ASC has said in the introduction to the documents, the Coalition does plan to create Objective Criteria and Best Practices documents in the future.

It is clear, however, that both users and anti-spyware software vendors are concerned about the deceptive EULA practices that mark spyware and other potentially unwanted technologies. EULAs, when used legitimately are an important agreement between consumers and companies, and users should read and understand these binding documents. EULAs can be used unfairly and deceptively, and the ASC does not condone these illegitimate uses.

October 27, 2005

Potential harms done by creating a standard definition

The most negative comments we received were from individuals who were skeptical about the utility of a standard definition of spyware. These comments seem to echo an article written by Brian Livingston, whose webpage included a link to the comment page.

The primary concern of these comments is that a definition of spyware and other potentially unwanted technologies will allow bad actors to construct programs that fall just short of the definition and will therefore be unflagable. One such comment reads:

I am concerned that this motion will actually play into the hands of spyware makers by giving them a clear line that they can stay just shy of and then use this to go about their noxious trade in impunity. What constitutes spyware is best left as an issue between anti-spyware makers and their customers: there is no need to formalize it.

(Olivier Lefevre)

This is a valid concern that ASC discussed in detail. However, it is ASC's contention the current Definitions has been written with the problem in mind, and leave plenty of room for individuals anti-spyware software companies to decide what fits their criteria for detection. The documents, in labeling problem technologies as "potentially unwanted," are an attempt to recognize that different consumers have different standards of unwanted programs on their machines. The ASC's biggest concern in the creation of these documents is consumer control over their computers and their user experience, and we have, therefore, avoided creating overly solid definitions that may impinge on consumers' market choices.

ASC continues to believe that the creation of a standard vocabulary for the anti-spyware software industry will not result in strict definitions that purveyors of spyware will be able narrowly avoid without significantly changing their bad behaviors. The primary result of these Definitions will be increased consumer ability to understand the differences among anti-spyware software and a better ability to make informed market decisions.

Individuals own definitions of spyware

Many individual users wrote into the ASC and gave their definitions of spyware. These definitions mirrored the concerns that other commenters have raised, and also mirrored the focus of the ASC in writing the Definitions. Each definition generally has a primary focus on one of three issues:

- User consent to installation and/or tracking

October 27, 2005

The term “spyware” because it has been used both broadly and narrowly in common parlance, the dichotomy was represented in the comments that presented simple definitions for the term. One commenter writes:

“Anything that is on your computer and sends information from your computer without your specific permission is to be considered spyware.”

(Anonymous)

While another individual comments that:

“The definition of Spyware should include ‘any program that installs itself surreptitiously on a user’s computer no matter what its purpose.’”

(Eliat B. Goldman)

- Simple, functional uninstall mechanisms

The second major characteristic that qualified a program as spyware is the absence of a simple and functional uninstall mechanism. Several commenters expressed sentiments similar to this one:

“The basic things that define unacceptable malware are that... (a) It conceals or disguises its activity, and (b) It does not come with a working uninstall utility...”

(Keith Tarrant)

- Deceptive representation of the purpose and function of programs

Only a few individuals who sent definitions of spyware directly mentioned deceptive practices, but it is worth noting that users have noticed that malicious programs are often installed under the guise of beneficial programs. One commenter defines spyware as:

“Anything that alters your browsing habits, or gathers data from you without your knowledge or under the disguise of bringing benefits to your browsing experience.”

(Paul Treneary)

All of the concerns represented in the definitions of “spyware” sent in by individuals are also present in the ASC Definitions and Supporting Documents. The goal of the ASC is primarily to protect the interests of consumers who find themselves grappling with the huge and ill-defined threat of spyware and other potentially unwanted programs. The ASC’s Definitions are an attempt to fully include all of these privacy concerns into one working definition of spyware that will ultimately help consumers make better market decisions about what anti-spyware software they use, and what programs they allow on their computers.

The very fact that so many individuals sent in varying definitions of spyware indicates that significant confusion does exist. The ASC’s aim in creating these documents is to

October 27, 2005

alleviate some of that confusion, while taking into account all of the privacy and security concerns that these individuals express in their definitions.

ASC made slight adjustments to the main definition. Most notably, we defined the term “technologies” in this context to apply specifically to “software and hardware components” based on a very welcome suggestion in a comment.

Negative comments against the coalition or specific members

These comments generally came from individuals who had had technical difficulties with a specific product or some other preexisting prejudice against a member of the coalition. These comments did not contain any productive suggestions or comments, and, therefore, do not require substantial response.

Other comments came from individuals who had specific complaints against certain members of the Coalition. The ASC is not a policing organization and exercises no control over its members’ internal practices. Each member of the coalition has been approved by the others as a legitimate anti-spyware software vendor or consumer interest group. Individuals with complaints against any organization should contact the company in question.

Confusion about the purpose of the document

Two comments questioned the direct impact that these documents will have on consumers and also the wisdom of starting the process by releasing definitions documents rather than documents like Best Practices or Objective criteria.

The ASC has been aware from its formation that the work that must be done to significantly reduce the threat of spyware and other potentially unwanted technologies is far more complex than can be accomplished in just one document. The ASC plans to follow the Definitions documents with several other projects including a Risk Modeling document and a Best Practices document, both of which will help to create standards that will enable consumers to better control their computers.

The ASC hopes to help consumers more effectively rid their computers of spyware and other potentially unwanted technologies by providing some coordination between anti-spyware software vendors that will enable consumers to make more informed market decisions about the products they use to maintain control of their systems. Defining the terms used in the dialogue between anti-spyware vendors and their consumers will help consumers better understand the differences among those products, and the different impacts that potentially unwanted programs may have on their systems.

The Coalition’s ultimate goal is to assist consumers in their struggle against unwanted and sometimes malicious actions. As ASC has said repeatedly in this process: the Definitions are not the final solution to the spyware problem, yet they are an important step in returning control of computer resources and personal data to the consumer.

October 27, 2005

Concerns about recognition and deletion of unwanted programs

Over a dozen comments came in from users with general concerns about their ability to recognize and fully delete any unwanted program on their computer.

These comments touch on a large issue that the ASC has tried to address in these Definitions. Users are primarily concerned about their ability to understand and control what happens to their computers. The Definitions and Supporting Documents do not specifically mention a user's ability to recognize and remove programs that they find to be unwanted, but the absence of an easy, functioning uninstall mechanism is a significant impairment of a user's ability to control a material change to their system and is therefore covered.

The driving motivation behind the ASC is to increase a user's ability to make informed market decisions about their computing experiences. This certainly includes a user's ability to correct any problems with system performance or distribution of personal information by removing programs that negatively affect those experiences. These issues will be addressed again in more detail in the objective criteria and other documents.

Interest in a risk modeling document

There were five comments specifically about the need for a risk modeling document. These commenters indicated that a system by which threat levels could be ranked would be a huge benefit for consumers trying to decide which programs to remove from their computers and which programs were beneficial. ASC agrees that such a risk modeling system would be valuable, and is currently working to produce one.

Definitions are too broad or too narrow

Several people commented that either the definitions were too broad or that they were too narrow. Both of these types of comments stem from the concern that the Definitions may have been written in a way that will allow bad actors to escape detection on technicalities.

Those who are concerned that the Definitions are too broad indicate that they fear that several different types of unwanted programs are absent from both the examples chart and the glossary, and will therefore go undetected. The ASC has written these documents with the specific goal of continued relevance as technology changes. The glossary and examples chart reflect the contemporary technical landscape, but classifying a program as spyware is not dependant on its specific inclusion in these documents. The Coalition believes that technology is always neutral and behaviors of individual programs determine how they are classified.

Another fear expressed is that such broad definitions could include software that is widely acknowledged as legitimate and would, therefore, undermine the definitions'

October 27, 2005

effectiveness. The ASC's response to this concern is that both legitimate and illegitimate companies can use these technologies. It is the effect these programs have on a user's control that determines whether a specific program is classified as potentially unwanted. These definitions will not create a shift in the kinds of programs that are flagged and labeled as potentially unwanted; they are simply a clarification and definition of the process by which a program will come to be detected by anti-spyware software.

Similarly, some commenters have indicated their fear that the definitions are too narrow and will be easily circumvented by bad actors. It is the hope of the ASC that these definitions will not need constant updating in order to remain relevant. As above, the documents do reflect today's technical context, but the classification of programs as potentially unwanted is independent of technical considerations. Rather, behavior is the focus of the definition. Spyware has become such a pervasive problem because it is often disguised and rapidly evolving. The ASC has attempted to define a framework that will allow anti-spyware software vendors and consumers to adapt to changing threats as quickly as new threats evolve.

Comments on the Vendor Dispute document

The comments specific to the Vendor Dispute Resolution document include two types of criticisms.

- The absence of users as a substantial part of the process of reevaluating programs that are detected.
- Concerns on the part of software vendors about the fairness of the proposed dispute resolution process.

The primary concern of those who indicated that they would like to see more user participation in the process was that various programs they consider unwanted could be reclassified or even removed from detection lists without public knowledge. This problem is easily addressed by anti-spyware software vendors publishing their detection lists on the internet. This was the subject of debate within the ASC. Different anti-spyware companies handle this issue in different ways for legitimate reasons and the group could not reach agreement on publishing as a best practice. In the end it was decided that each anti-spyware company interacts with its customers in different ways, and, ultimately, consumers must make a market decision based on the choices and information available to them. ASC encourages consumers who feel strongly about this issue one way or another to make their decisions known in the marketplace.

The second concerns were raised primarily by software vendors who were concerned that the proposed vendor dispute resolution process may be structurally unfair to their companies. These companies listed seven primary concerns:

- that the time limits set for an anti-spyware vendor to respond to a complaint were undefined;
- that the time limit example given for resubmission of a complaint was too long;

October 27, 2005

- that confidential business data submitted in the process of review needs to be kept securely or not kept at all;
- that a company not be required to provide a full list of distributors, but rather just some individual examples of distribution mechanisms;
- that anti-spyware vendors should provide final decision-making in writing;
- that neutral arbitration be provided if parties are still in disagreement; and
- that detection criteria be made available to the public.

The first and second complaints (on timing) have been addressed by the removal of the example of a 90-day waiting time for resubmission and the addition that all response and resubmission limits must be reasonable. Individual companies have different technical and administrative constraints that affect the time periods for responses to complaints and the limits they place on resubmissions. For this reason, the ASC does not give specific temporal requirements to vendor dispute processes. However, the fear that anti-spyware companies have no incentive to review complaints from software companies is a legitimate one, and the ASC does clearly indicate that reasonable efforts must be made to resolve software disputes in a timely manner.

The ASC acknowledges the real concerns about security of confidential business information. The Coalition suggests that anti-spyware vendors will want to have a policy on accepting and storing confidential business information. However, because of the range of types of anti-spyware vendors, their different markets and aims, the Coalition was not able to develop best practices for these policies. In any case, it is incumbent on the software publisher to read these policies and mark confidential business information accordingly. If confidential business information is received, anti-spyware vendors should submitted in a complaint be securely stored and kept only as long as necessary for administrative, legal, or technical reasons. As protocols in the vendor dispute process develop ASC may revisit this issue again.

Similarly, some companies indicated that providing a full list of distributors and affiliates may not be possible, and request that providing only specific examples of distribution methods will be considered sufficient. Unfortunately, there is no way for an anti-spyware software company to determine if a software company is following good practices unless a full distribution list is provided. Any application that does not contain a full list of distributors may be considered incomplete.

The ASC thought that it had clearly stated that the entire process should be in writing, but comments suggesting that the final decision-making rationale should be included pointed to the fact that ASC did not do so in enough detail. Changes have been made to the document to address this concern by clearly stating that this is a best practice.

It was also suggested that software publishers who are not satisfied with a review should be able to pay for neutral arbitration as an appeal. ASC does believe that there are indeed rare cases neutral arbitration may be necessary and encourages companies that are at an impasse to discuss neutral arbitration as an option. While some may suggest that anti-spyware vendors have no reason to enter into an arbitration process on their own since

October 27, 2005

they are reviewing their own past decisions, ASC wholeheartedly disagrees. In fact, depending on the market and legal situation there are circumstances where an anti-spyware vendor may call for a third party to run their entire dispute process (this has been noted in the new draft of the dispute resolution process document). Yet, arbitration can be a time and resource burden on all those involved, even in cases where only one party is paying the arbitrator. Arbitration can also be used as a tool to drag out a process that has clearly been correctly decided. Therefore, ASC believes that arbitration must be a decision entered into through an agreement by both parties.

Finally, the desire that detection criteria be made public is similar to the desires expressed by consumers that detection lists and criteria will be made available to the public. As with the consumer concerns, the publication of detection criteria is a business model choice made by individual companies, and will have to be subjected to market pressure and choice by consumers. Some companies may publish their detection criteria and others may determine that these criteria constitute business information that they do not wish to publish. On a related note, one of ASC's next goals is to publish considerations for criteria that will include a general set of detection criteria. We hope that this document will give individuals an idea of the broad set of criteria that individual anti-spyware vendors may choose include in their own criteria.

Specific edits and suggestions

A significant number of comments were specific line edits and vocabulary suggestions for the document. The content of these comments was quite varied, but can be further broken down into several categories.

Concerns about the definition of the term "spyware and other potentially unwanted technologies"

There were a couple of comments that suggested that the grammar of the primary definitions of spyware and other potentially unwanted technologies was unclear and that the syntax needed to be reworked. In response to this concern, we have slightly changed the language of the definition. The content and import of the definitions has not been changed, but the language has been slightly altered to make the relationship between the different parts of the definition more clear.

Concerns about the neutrality of technology definitions

The ASC has tried to indicate in its Definitions and Supporting Documents that technologies are neutral until they have been given bad behaviors that make them unwanted. Some comments express concern that some of the technologies in the examples table and in the glossary are not described neutrally.

In particular, ASC has created a definition of "underlying technology" and added all of the underlying technologies mentioned in the document to the glossary based on several comments.

October 27, 2005

It is important to note that all technologies exhibit some behaviors at a base level, and the ASC has attempted to break those behaviors down to the minimum level that would cause a program to be classified as a certain type of technology. However, the chart and the glossary provided are attempts to clarify the definitions of terms in the common anti-spyware parlance.

Specifically, some commenters — particularly those in the advertising industry — objected to the definition of “adware.” The ASC has designated advertising supported software as a neutral technology and nuisance or harmful adware as the potentially unwanted incarnation of ad serving software. Adware is a definition that fell into a gray category. ASC was trying to make clear that not all adware is necessarily unwanted, but that anti-spyware vendors may want to make users aware of particular adware programs since they “may potentially” be unwanted. It was the strong feeling of the Coalition and many commenters that to completely over look the unwanted potential of adware would be to write an incomplete definition of spyware.

The second significant comment we received about neutral definitions was from Macromedia, who objected to the ASC’s definition and use of “Flash.” Macromedia indicated that the current definition of flash was incorrect and incomplete, and that several proprietary technologies were mentioned by their product name with no mention of the affiliated company. In light of these comments, the ASC has changed the definition of Macromedia Flash to more accurately reflect the technical reality, and has added company names to all proprietary technologies including changing the term “PIE” to “United Virtualities Persistent Identification Element (PIE).” ASC removed the definition of Macromedia Flash, because it was tangential to the issues at hand. The Coalition believes that the other changes from Macromedia make the glossary more accurate, and do not represent a substantial change in the content of the document and thanks Macromedia for calling them to our attention.

Use of notice, consent, and control as criteria for defining unwanted programs

Several of the concepts introduced in the Definitions document are dependant upon the phrase “notice, consent, and control.” The ASC, in asserting that technologies are neutral and only bad behaviors will cause a program to be classified as “potentially unwanted” is attempting to recognize that the essential problem of spyware and other potentially unwanted technologies is a loss of consumer input and control over their computer’s resources and data. These documents do not currently contain a definition of notice, consent, and control, but it has been and remains the intention of the Coalition to publish other documents such as an objective criteria document, and a best practices document in which the standards of notice and consent will be discussed in more detail.

It is the opinion of the Coalition that the problem of spyware is too complex for a consensus building organization to attempt to solve all at once. These Definitions mark an important first step in the battle against spyware, but they do remain just the first step

October 27, 2005

in the process of establishing standards for consumer protection against spyware and other potentially unwanted technologies.

Concerns about the inclusion and definitions of cookies

Several commenters indicated that they were uncomfortable with the inclusion of cookies in the same category as other, potentially more harmful technologies. The ASC defends its inclusion of “tracking cookies” as potentially unwanted technology, since many consumers have voiced concerns about the use of cookies for unwanted purposes.

All of the programs and technologies that are classified as “spyware and potentially unwanted technologies” are not automatically unwanted. With proper user control, these technologies can be valuable to consumers. One commenter indicated that the cookie controls in Web browsers allow for user control over the installation of cookies on their machines. This is true, but these cookie controls are a separate program used by consumers to control what is installed and stored on their machines. They are not user controls built into the technology itself. Therefore, the ASC sees very little difference between using a browser or anti-spyware software to control which tracking cookies are planted on a computer. Both of these methods serve to give the end user control over his or her browser experience.

Miscellaneous

Some advertising companies were concerned that the ASC was not an inclusive forum. ASC is comprised of the leading anti-spyware companies and distributors and interested consumer and public interest organizations. All members must be approved with complete consent of all other members. The standards for participation were designed to ensure that the important dialog among these interests could be open and fruitful. ASC recognizes that it is difficult for public interest groups to participate in the process and has made several outreach efforts to include consumer groups that do not focus on spyware and are not members of ASC, into the discussion. Several public interest groups including CAUCE Canada and the National Center for Victims of Crime have joined the group since the comment period began. Consumers Union and National Consumers Law Center also participated in one of the closed meetings that the group held. The open comment period was also an attempt to include more voices in this process. ASC also briefed many groups, including advertisers on the documents during the open comment period. While ASC will continue to look to work with different communities and create new avenues for openness, the Coalition feels strongly that, to date, its process has actually been one of the most open of any collaboration between members of the technology industry and public interest groups.

There were also many other specific edits suggested by commenters, and all of these suggestions have been taken under consideration by the ASC. Often, these comments helped us to correct typos, spelling errors, and grammar issues that often arise in documents written with a large group. Other comments were helpful in clarifying the meaning and intent of the definitions. While we are greatly indebted to the commenters

October 27, 2005

involved, the comments did not affect the general meaning of the document, and so, do not require individual discussion here.