

Best Practices: Guidelines to
Consider in the Evaluation of
Potentially Unwanted
Technologies

Introduction

In October 2005, the ASC released its Working Report -- Definitions and Supporting Documents, which defined the term "Spyware (and Other Potentially Unwanted Technologies)." One of the key tenets underlying that definition was that it was ultimately up to the user to determine whether a technology's behavior is wanted or unwanted. A piece of technology that exhibits behaviors unwanted by users in one context may offer enough benefits that it becomes wanted by the same users in another, particularly if the technology in question is offered with proper notice, consent, and user control. The report offers a table documenting types of underlying technologies and short descriptions of reasons why a certain implementation of an underlying technology may be wanted and why a different implementation of the same underlying technology may be unwanted.

In January 2006, the ASC broadened the explanation of what makes certain technology implementations potentially unwanted with its Risk Modeling Description, which detailed the criteria by which anti-spyware companies classify Spyware and other Potentially Unwanted Technologies. These criteria include both risk factors – those that increase the potential concern about a technology – and consent factors, basic notice, consent, and user control – that mitigate the risks.

While these documents offer a transparent picture of how anti-spyware vendors and researchers consider negative and positive behaviors, the ASC believes that it is important to move past the current behaviors and to help create a better marketplace. To this end, the ASC drafted this Working Report of Best Practices to highlight the sorts of technological behaviors that limit the negative impact of potentially unwanted technologies. This Working Report is designed for use by anti-spyware vendors, but contains important insights for many software publishers as well.

Except where noted, these best practices are written with the assumption that users and customers will be adults. In cases where children or teens are the targets of a particular technology or software, more stringent requirements may be necessary, particularly in areas of giving notice and receiving consent. Some legal jurisdictions may also have laws in place regarding dealings with minors, but publishers seeking to follow best practices must sometimes go above and beyond those laws.

Scope

The goal of this Best Practices document is to further explain the consent factors described in the Anti-Spyware Coalition's Risk Model Report. While the main audience for this document is anti-spyware vendors, ASC believes that it will also aid publishers of potentially unwanted technologies to make their products less harmful and more desirable to users, and therefore will benefit users, software publishers and anti-spyware developers alike.

Within the Anti-Spyware Coalition's Definitions document, a number of technologies which are considered "potentially unwanted" were described. This document is aimed at providing best practices suggestions for publishers of software that use these technologies. For reference, the behaviors underlying those potentially unwanted technologies are listed below:

- Tracking
- Advertising display
- Remote control
- Dialing
- System modifying
- Security analysis
- Automatic download
- Passive tracking

This document contains numerous terms, such as “personal information,” which are defined in the ASC’s Definitions document (<http://www.antispywarecoalition.org/documents/index.htm>).

The practices are written either specifically as issues for anti-spyware vendors to examine, in which vendors are mentioned explicitly, or as policy criteria for vendors to consider, which are listed by the behavior of the software.

Finally, it is important to note that this is not a final document. As with all ASC documents, it is intended to be revised from time to time as new threats arise, and as perceptions change about proper behavior. Also, because this document is designed for use by anti-spyware vendors, publishers engaging in potentially unwanted behaviors should also, where applicable, consult other best practice documents that will be more focused on development of their products when making determinations about building consent practices for their software.

Compliance and Certification

In general, the ASC Risk Model offers a normative set of objective criteria, whereas this document is designed to provide an aspirational set of policy criteria. Publishers should refer to the ASC Risk Model to understand the balance of Risk and Consent factors and how they may apply. **In either case, it is important to note that a publisher’s adherence or reference to this document in no way guarantees that the publisher’s technology will or will not be classified by members of the ASC as spyware.**

This document is not the basis for a certification program. It offers best practices – suggestions – both for anti-spyware vendors to use in making determinations in their evaluation of software and for publishers to consider in the developing of their products. Readers seeking more concrete guidelines that are accompanied by actual certification programs are encouraged to seek out other organizations in this space that perform this function. Some ASC members are also members of various other certification bodies, and some are not, but the group as a whole does not intend to perform this function.

In addition, publishers should follow the law in jurisdictions where they operate. There will invariably be cases where the law addresses concerns that this document does not, or where there may be differences between ASC recommendations and specific laws of some jurisdictions. In such cases, publishers should always follow applicable laws.

Outline

In this paper, we outline the best practices for publishers of potentially unwanted technologies, giving guidelines for the following:

- Value to the User
- Notice
- Consent and control
- Security
- Redress

The first part of the paper will detail best practices that are applicable to any type of potentially unwanted technology. The second part of the paper will provide best practices for the types of underlying behaviors of potentially unwanted technologies listed in the previous section.

Best Practices for All Types of Potentially Unwanted Technologies

Value to the User

Anti-Spyware vendors may evaluate the steps that a software technologies publisher has taken to provide prospective users of a product with a specific value inherent to the product. In much the same way that consent offsets risks raised by a certain piece of software technology, value offers the user a reason for downloading or installing a piece of potentially unwanted technology. Ultimately, users will make the decision whether or not they want a particular technology, but following these best practices will help create a more robust marketplace for users to make decisions.

Expectations about Value to the User

- All software technology sold or given away for free should offer value to users;
- The value of the software technology to all impacted users should outweigh the risks posed by the software technology;
 - In evaluating the business model of a particular piece of software technology, a publisher should examine the balance between value provided by software technology in terms of usefulness, necessity and entertainment vs, the potential harm or annoyance that the software technology could cause, such as through dissemination of personal information, through the display of advertising or degrading of internet connectivity

(For example, the value provided by a simple screen-saver may not outweigh the annoyance of the ads supporting it, while a full-featured email client or web browser may provide sufficient value to justify such ads).

Notice

Users should be notified in simple, clear language about the nature of the software technology and the Web site¹ with which it may be associated.

Notice Expectations

- Anti-spyware vendors may evaluate whether the publisher of the software technology has identified themselves on their web sites and provided information about their policies, including accurate, accessible and complete contact information;
- Anti-spyware vendors may evaluate whether the publisher has provided users with accurate details of the software technology in a time place and manner that is useful to the user. This includes:
 - a description of the software technology and what it does;
 - a description of any third-party software components that will be downloaded or bundled with the primary software technology; and
 - accurate version information of the software technology.
- Anti-spyware vendors may evaluate whether the publishers have presented users with an End User License Agreement (EULA) prior to installing software technology that describes the terms and conditions or use of the software technology. The EULA should be accurate, easy to access, save and print. It should be written in clear, concise language;
- Anti-spyware vendors may evaluate the extent to which:
 - files have easy-to-understand names and are easy for users to find on their computers.
 - the location where the software technology is to be installed can be easily changed by users and whether such a change is appropriate considering the application;
- Anti-spyware vendors may evaluate whether publishers have digitally signed their code and content files. The code signing certificate becomes part of a chain of certificates leading back to one certificate (sometimes called the root of trust). Certificates have a higher level of effectiveness if they are chained to a root of trust. The purpose of a certificate chain is to guarantee each component's integrity and identity, and act as an assurance to the end user and other security software that the content is safe, truly comes from the publisher's organization and hasn't been altered in transit.

¹ When the term "Web site" is used or reference is made to the content of a web site in this document, unless explicitly stated otherwise, the term refers only to the web sites of publishers of potentially unwanted technologies, or services that may contain such technologies.

Anti-Spyware Coalition

- There should be a clear indicator when the program is active. For example, the user interface, an icon, or some other easily noticed indicator should show that the program is running;
- Users should be clearly informed of material implications the use of the software technology has on their privacy, security, and overall computing experience. This includes any collection of information about them and any known adverse impact on their computers caused by running the software technology;
- Anti-spyware vendors may evaluate whether the software technology publisher or related web site has provided a readily accessible, accurate, easy-to-understand privacy policy that fully explains its data collection, use, and disclosure of data about users:
 - The privacy policy or Statement should disclose all information required by law and should address fair information practice principles;
 - The privacy policy or Statement should be concise and written in easy-to-understand, straightforward language. Users should be able to access it, save it and print it at any time; and
 - To ensure the readability of the privacy policy, a layered approach may be taken by a publisher, in which the first content encountered by the user explains the policy in broad terms that are easily understandable, and the legal details of the policy are revealed on further pages.
- Anti-spyware vendors may evaluate the extent to which the notice provided has been written appropriately for an intended user's age and reading ability. In general, if the intended users of a piece of technology are minors and/or children the language used in privacy policies and other important documents should not exploit the credulity, lack of experience or sense of loyalty of children.

Prominent Notice

In general, anti-spyware vendors may evaluate the extent to which the notice should be provided in a prominent, direct way before a program does anything that has material implications for user privacy, security, and computing experience. This includes, but is not limited to notice about:

- Collecting or sharing personal information about users;
- Tracking Web surfing behavior for purposes that a user may find unexpected or unwanted (such as tracking outside the context of the software owner's application);
- Delivering disruptive advertising, for example pop-up advertising outside of the web page;
- Initiating an unauthorized and/or clearly unexpected outbound connection (modem, network, Bluetooth, Infrared, etc.);
- Modifying settings on user computers such as home page, security settings, toolbars, menus, etc.;

- Bundling other software programs with a program that users have chosen to download; and
- Automatically updating software that installs new versions that materially change behaviors.

A prominent notice can be delivered through a number of means, including a well-defined, required step in the installation process; a window that alerts users to what is about to occur; or some other direct, noticeable, and easily understood means. The required visibility of the notice will vary with the context. The prominent notice should cover answers to the questions under the “Notice Expectations” section. If it doesn’t provide the details to answer these questions directly, it should provide a way to access these details, for example, through a “learn more” button to a more complete notice.

Consent and Control

Users should be in control of their computers at all times. Anti-spyware vendors may evaluate the extent to which the software technology publisher has asked and received consent from the user before performing activities such as installation or uninstallation, or the collection, use or disclosure of personal information. For potentially unwanted technologies, EULAs alone are usually not enough to offset risk behaviors. Individual consent of risky behaviors may be appropriate.

Consent Expectations

Potentially unwanted technologies should ask for user consent before software technology is installed or uninstalled, or if any personal information about users will be collected during software technology installation or when the software application is running. After providing a prominent notice about what is about to occur, users should be presented with a clear, easy-to-understand choice. For the consent to be meaningful, the purposes for which the information is being collected and will be used should be stated in a matter reasonably understandable to the user. Nothing should happen unless users provide a clear, affirmative “Yes” to whatever is proposed. If users choose not to agree, there should be no disruption or interference with the computing experience. There should not, as a condition to the supply of a product or service, be a requirement for a user to consent to the collection, use, or disclosure of information beyond what is required to provide the services or applications in question without clear choices for the user.

Proper consent can be obtained in a number of different ways. For example, consumers may be required to:

- Click a link that clearly specifies what the consumer is authorizing by clicking (e.g., "Download Now");
- Click "OK" to a prominent notice that clearly describes what the consumer is authorizing by clicking “OK”;
- Enter personal information in a form and clicking "Submit", after having reviewed and agreed to the relevant policy explaining how the information will be used; or
- Read a EULA (scrolling through) and click "I Accept", after having an opportunity to save and print the EULA.

Anti-spyware vendors may consider the impact on the user in making determinations about the adequacy of the consent mechanism. Consent should not be obtained through deception or omission. In obtaining consent, the reasonable expectations of the user are relevant.

If any event is about to happen that would require a prominent notice (see Notice section), the default choice should either be set to "No" or there should be no default selected. An example of these types of events include when additional software technologies are going to be bundled with the software being downloaded. The form of consent sought by the publisher may vary, depending on the circumstances and the type of information. Anti-spyware vendors should consider the sensitivity of the information collected or transmitted when determining whether publishers have offered the appropriate level of notice and consent.

When evaluating programs designed for use on operating systems that allow for the creation of multiple "accounts" on a single computer, anti-spyware vendors may evaluate whether the publisher has required consent from each individual account during the first interaction with the application, or from an administrator account on a managed system, where appropriate.

Anti-spyware vendors may evaluate whether the publisher has offered users a reasonable mechanism for removing and deleting personal information (subject to legal enforcement or fraud-related issues).

Anti-spyware vendors may evaluate whether publishers have taken reasonable steps to prevent monetary transactions with children and should be aware that under most jurisdictions, minors and/or children under a certain age are deemed to be unable to give consent. In cases where this document requires consent and a minor is involved, express consent from a parent or legal guardian should be obtained. Many countries have laws regulating commercial dealings with minors and publishers should follow them.

Control Expectations

After users consent to installing and using a software program, Anti-spyware vendors may consider the extent to which users are able to easily control the software technology. This includes:

- **Creation of launch mechanisms**

Where an application intends to create duplicative launch mechanisms (for example, shortcuts), anti-spyware vendors may consider the extent to which the installation procedure allows the user to opt-out of individual mechanisms.

Anti-Spyware vendors may also consider the creation of launch mechanisms for software applications and web sites other than those reasonably expected by the user.

- **Control of automatic startup of programs**

Programs that wish to start automatically should offer the choice about such behavior.

- **Starting, stopping, closing, and removing programs**

Users should be able to start, stop, and close the software program at any time that they choose. Programs should follow standard known methods for installation and uninstallation (such as the “Add/Remove Programs” feature in operating systems).

- **Uninstallation of programs without difficulty**

Programs that users uninstall should stay uninstalled. Uninstallation should not have an adverse effect on the computer. If uninstalling software will impact the performance of the computer or other programs, then prominent notice should be provided to users prior to software technology uninstallation. Anti-spyware vendors may consider the extent to which all components of a software program have been removed and the potential impact of any components left behind.

- **No unwanted interference with Web browsing**

When users search and/or access web sites, there should not be any interference by third parties to whom the computer’s user or administrator hasn’t given permission. Search results or web page content should not be modified by another site or publisher.

- **No nuisance behavior or unreasonable impairment of user productivity.**

Users should expect software technologies to avoid impairing productivity including slowing down the user’s computer or causing crashes and/or loss of data.

- **Giving users control over their personal information.**

Users should be able to determine what personal information is collected from them and how that information is gathered, used, and communicated to others.

In particular, anti-spyware vendors may examine the extent to which the publisher has:

- published and made readily available to users specific information about their policies and practices regarding the collection, use and disclosure of personal information;
- specified, up front, the purposes for which they collect personal information, and should limit such purposes to those that a reasonable person would consider appropriate in the circumstances;
- limited their collection of personal information to that which is necessary for the purposes they have identified and communicated to users;
- collected personal information only by fair and legitimate means;
- not collected personal information indiscriminately – the amount and type of information collected should be limited to that which is necessary to fulfill the reasonable purposes identified by the publisher;
- retained personal information only as long as necessary to fulfill these purposes;

- made efforts to ensure that personal information that is no longer required to fulfill the publisher's identified purposes or other legal constraints is destroyed, erased, or made anonymous and whether the publisher has developed and is enforcing minimum and maximum retention periods for personal information;
- only updated information, personal- or computer-related, where such a process is necessary to fulfill the purposes for which the information was collected; and
- provided the ability to users to access and correct personal information about themselves held by the publisher, where reasonable, upon request through a quick, easy and free mechanism.

Electronic Mail

The questions surrounding the marketing to consumers using electronic mail are complex and outside the scope of this document. Publishers are encouraged to seek out and follow existing best practices regarding commercial electronic mail such as those developed by the Canadian Task Force on Spam² or the OECD Task Force on Spam³.

Security

Any software technologies that users download should maintain the security state of their computers. This includes maintaining security in the transmission of data and not interfering with:

- Security applications, for example, anti-virus, anti-spyware, or firewall software;
- Application or browser security settings;
- Internet connectivity security; or
- Operating system security settings.

In the process of evaluation of software technologies, anti-spyware vendors may seek to ensure that Web sites, software publishers, or other third parties have not interfered with the secure encryption, authorization, and authentication of user data when users do business on the Internet.

Software technologies should not have a significant negative impact on the overall security of the system without the user's consent.

All information collected, especially personally identifiable information, should be protected with security safeguards appropriate to the sensitivity of the information. This includes the use of appropriate security safeguards during transmission, storage, or destruction of the information.

² See <http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/gv00330e.html>

³ See http://www.oecd-antispam.org/article.php3?id_article=265

Redress

Anti-spyware vendors may take into consideration the extent to which the software technology publisher or web site provides a valid company name, mailing address, phone number, web site address, and email address so that users can contact the company with any questions or disputes about the software technology. Vendors may also seek to ensure that the company in question has taken responsibility for their own privacy policies and for the timeliness and completeness of their response to complaints.

Accountability

Anti-spyware vendors may take into consideration the extent to which the publisher and related organizations have taken responsibility for the personal information in its care and whether they have named someone who will be accountable for compliance.

- In cases where others are responsible for the actual collection of personal information, it should still be assumed that the designated person is accountable,
- Anti-spyware vendors may also seek to ensure that the designated contact for a publisher responds to user inquiries in a complete and timely manner.

Communications to Users

Anti-spyware vendors may take into consideration the extent to which:

- Responses to user contact are timely, with regard to the urgency of the user contact;
- Responses to user contact are informative, relevant and complete;
- Responses include correct and relevant contact information so the user may carry on further communication;
- There is a pre-defined escalation plan available to users if responses are unsatisfactory and a clear process for informing users how to invoke that plan; and
- The user has access to adequately and effectively trained staff and support.

Best Practices for Specific Types of Potentially Unwanted Technologies

The following best practices apply to specific types of potentially unwanted technologies, and are supplemental to the best practices outlined above.

Tracking Software: Keyloggers, Screen Scrapers, and Remote Monitors

The nature of tracking software is such that anti-spyware products will always want to detect tracking software. The following practices will build trust and reduce the perceived

threat. While a reduced threat will not likely change the detection policies of anti-spyware software, it may greatly influence the default remediation policies.

Value to the User

Benefits to the customer might include:

- prevention of hacking through active monitoring;
- measuring productivity (corporate use);
- policing leakage of private information (corporate use);
- recording computer activity;
- monitoring youth chat/email (home use); and
- keeping a record of everything a user types or does online.

Consent and Control

Tracking software is generally installed with the consent of the party initiating the surveillance, but not necessarily the consent of the party being monitored. This can lead to an invasion of privacy and even illegal activity. This section is dedicated to changing this practice by illustrating ways of notifying the party being monitored.

It is vitally important that users are aware of surveillance. Anti-spyware vendors may consider how a publisher displays prominent and regular notification and to what extent the notice includes or references the information being tracked, by whom and for what purpose.

Security

Tracking user activity can gather sensitive information that can be damaging to both the monitoring party and the monitored party. A best practice for tracking software is to protect that information through a strong encryption mechanism. This way, the monitoring party can be confident of the origin of the tracking information, and only the monitoring party can access the tracking information. Anti-spyware vendors will want to take these issues under consideration.

Advertising Display Software

In general, advertisers should follow standard industry practices for truth and honesty, avoiding the presentation of false or deceptive content.

To respect user privacy, advertising display software should not display objectionable language and/or content.

Perception of objectionable language and/or content is very subjective and each user will interpret content differently, so avoiding any content that might be questionable, depending upon context, is a best practice.

Value to the User

The value inherent in Advertising Display Software is based upon the intrusiveness of the advertisements served as balanced by the value of the bundled software itself. Anti-spyware vendors may consider whether publishers have endeavored to maximize the value that user gets from the bundled software, while minimizing the intrusiveness of the advertising served.

Notice

Anti-spyware vendors may consider:

- Whether notice includes information about the advertising that will be displayed, if the advertising is not directly triggered by the user's interaction with the application, or if the use of any other application is disrupted by the ad.

Including a sample of such an advertisement in the notice allows the user to easily identify the advertising displayed by the software. It's a best practice to also identify the format in which the advertising will appear (pop-up, slide over web page, etc.) and to give an estimate as to how often the software will display advertisements.

- When an advertisement such as above is displayed, whether users are able to clearly identify the program that is generating the advertisement and the programs with which the ad-serving was bundled. Advertisements that are part of a web page or identifiable within the main window of the responsible program fulfill this requirement.

Consent and Control

Anti-spyware vendors may consider:

- Whether advertising display software installed at or through web sites intended for children provides for parental notification and consent for installation of the software;
- Whether users are provided with an easy way to control advertisements;
- Whether users are able to close the advertisements quickly and easily, for example, by simply closing a pop-up or quitting the program; and
- Whether users are also be able to quickly and easily stop and/or uninstall the program that delivers the advertisement.

Remote Control Software

Notice

- Remote Control Software should prompt the user to accept incoming control from another person, using clear notice, with positive assent required;
- Remote Control Software should display a clear notification prominently on the user's screen during the entire time that the remote control software is active, whether or

not the computer is under another person's control. There may be a different or an additional notification displayed when the computer is under another person's control. If no user is in control of the computer (i.e. – the computer is logged out or "sleeping"), notification should be made at the next available opportunity; and

- Remote Control Software should keep a log of remote accesses in an easily found location.

Consent and Control

- Remote Control Software should only be installed with the active consent of the user of the computer. During installation, the user should be clearly informed about the purposes of the software, including the fact that the technology will allow other people to control various aspects of the operation of the computer while the software is operational;
- Remote Control Software should not automatically arrange to launch at start up of the user's computer. Only through the direct action of the user should others be allowed to attempt to control the computer;
- Users should be able to easily disconnect another person from controlling their computer through use of a key stroke or mouse movement;
- For the user's consent to be meaningful, there must be reasonable robust authentication scheme ensuring that the person remote controlling the user's computer is the person actually authorized by the user; and
- Remote control software should have adequate encryption capabilities to protect against unauthorized monitoring or tampering with a legitimate remote control session.

Dialing Software

Notice

- Dialing Software should be clearly disclosed to the user prior to installation of the Dialing Software itself, or any application package the Dialing Software is bundled with;
- Unless a user has expressly consented to a flat-rate billing plan, during the duration of the call, Dialing Software should display a clear indication prominently on the user's screen showing the number connected to and the current duration of the call; and
- Dialing Software should, by default, not mute the speaker on the modem.

Consent and Control

- Dialing Software should only launch when required to dial a number at the request of the user. At times when it does not need to be active, it should not be running;

- Dialing Software should not dial any number not requested by the user or required to connect to a service requested by the user;
- Before dialing any number, Dialing Software should display the number to be dialed to the user and obtain active consent before placing a call. Anti-spyware vendors will want to consider the extent to which a user is provided with prominent notice of the list of numbers to be dialed or a number is dialed in place of a number indicated by the user, in order that the user can avoid toll charges; and
- Dialing Software should provide a clear and easy to operate mechanism for disconnecting a call at any time.

System Modifying Software

Value to the User

- System modifying tools should offer a user the opportunity to customize the operating system to release some extra value. Such a value may take the form of faster processing or better disk access or a similar enhancement.

Notice

- It should be made clear before the user installs the software that an application needs to change a setting in order to run. This notice should follow the informed consent process described earlier in this document.

Consent and Control

- If the user elects to uninstall this application, then the uninstall procedure must allow the restoration of all system changes to their previous values or conditions, except when doing so would create undue burden or other risk to the user; and
- When an application wants to change Internet browser settings such as the home page or the search page or the 404 (site not found) message, then the user must have the option to specifically authorize these changes. Anti-spyware vendors may consider the extent to which the application allows a user to restore their previous settings;

Security Analysis Software

Value to the User

- Security Analysis Software should be marketed in such a way as to discourage unwanted or harmful use of the program; and
- When searching for system vulnerabilities, the Security Analysis Software should inform the user of the nature of discovered vulnerabilities and how best to address them, but should not assist the user in taking advantage of any vulnerability discovered.

Notice

- Security Analysis Software should display prominent notice while running.

Consent and Control

- Security Analysis Software should only be voluntarily installed with the knowledge of the owner of the computer. During installation, the user should be clearly informed about the purposes of the software, including the possible threat to computer security that it poses;
- Security Analysis Software should require administrator access on the operating computer to install and to run; and
- When possible, Security Analysis Software should require administrator access on the computer that is the target of a scan in order to perform the scan.

Automatic download software

Value

- Automatic Download Software should allow the user to easily procure desired applications and updates to previously installed applications.

Notice

- Anti-spyware vendors may consider the extent to which Automatic Download Software has informed the user, with prominent notice, when a download is about to take place or provided clear consent approving downloads without such notice (as discussed below); and
- The user should be informed upon installation of the software that the software is designed to automatically download.

Control and Consent

- Anti-spyware vendors may consider the extent to which publishers provide options to require notice/consent prior to download occurring or to allow the Automatic Download Software to operate in the background without interaction; and
- Automatic Download Software should never install downloaded items without prior active consent by the user; and

Security

- Automatic Download Software should verify integrity of downloaded packages before installing. As in other areas, anti-spyware vendors may take the materiality of the update under consideration (e.g. – security updates or network centric updates).

Passive Tracking Technologies

Notice

- All domains should contain a full P3P policy (Platform for Privacy Policy Project)⁴ and individual cookies should contain a compact P3P policy that accurately gives notice of their data collection, use and sharing activities and contains a link to the full policy.
 - The full P3P policy should contain a link to the privacy policy of the data controller.
 - The full P3P policy should contain a general description of the data controller's data retention policy.
 - The full P3P policy should clearly state whether PII (personally identifiable information) is being collected and if this is being shared with a third party.
 - If data is being shared, clear disclosure should be provided with a link to the third party's privacy policy.
 - If an opt-out is available to the end-user, this should be communicated in the full P3P policy and be easily accessible from the data controller's privacy policy.
- If an opt-out is available to the end-user, the data controller must provide a programmatic method for the users to communicate their choices. Anti-Spyware vendors may consider the extent to which requesting that the end-user change their browser options is or is not considered a valid opt-out.
- If a site permits a third party to use a cookie to collect data for use in tracking or targeting on unrelated websites, Anti-Spyware vendors may consider the extent to which the privacy link on the site includes a reference to the use of cookies and a link to the 3rd party's privacy policy.
- Companies that primarily do business through third party ad networks or marketing affiliates should ensure that the home pages of their sites include prominent notice, visible without any need for scrolling on most computers, that links to data practices associated with the cookie.

Consent and Control

- No third party tracking cookie should have a lifetime of more than an expected and reasonable use and no longer than two years from the most recent interaction with the data controller.
- A passively tracked document that uses unique IDs embedded in a common file format should be opened only with the active and informed consent of the user of the computer.
- Active and informed consent should be obtained every time the user opens a passively tracked document that uses unique IDs embedded in a common file format.

⁴ See <http://www.w3c.org/p3p/>

Security

- Cookies should not themselves contain personal or sensitive information.
- If sensitive information is gathered through a passively tracked document that uses unique IDs embedded in a common file format, it should be protected through a strong encryption mechanism.