An Introduction to P3P

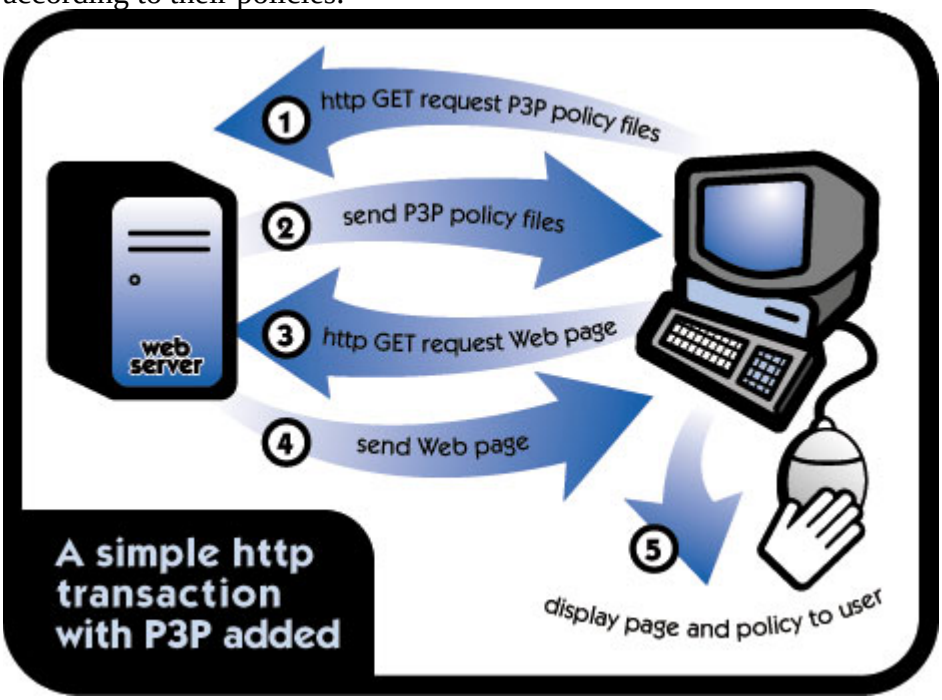
From Platform for Privacy Preferences Project, http://www.w3.org/P3P/

1. What is the Platform for Privacy Preferences Project (P3P)?

The Platform for Privacy Preferences Project (P3P) is an automated way for users to gain more control over the use of personal information on Web sites they visit.

At its most basic level, P3P is a standardized set of multiple-choice questions, covering all the major aspects of a Web site's privacy policies. Taken together, they present a clear snapshot of how a site handles personal information about its users. P3P-enabled Web sites make this information available in a standard, machine-readable format. P3P enabled browsers can "read" this snapshot automatically and compare it to the consumer's own set of privacy preferences. P3P enhances user control by putting privacy policies where users can find them, in a form users can understand, and, most importantly, enables users to act on what they see.

Although P3P provides a technical mechanism for helping inform users about privacy policies before they release personal information, it does not provide a mechanism for ensuring sites act according to their policies.



2. Does P3P allow you to send personal data to a site without human intervention?

No. The P3P guiding principles state that P3P user agents should "not be configured by default to transfer personal information to a service provider without the user's consent."

3. Does P3P require new server software?

No. P3P 1.0 uses the normal HTTP 1.1 protocol for the exchange of policies, and the matching of policies to user preferences takes place on the client-side. Thus, P3P can be enabled on Web sites that use any HTTP server.

Regular users have coverage for P3P through setting configurations in Internet Explorer 6.0.

Web sites can post/implement their P3P settings on their servers by translating their human-readable privacy policies into P3P syntax and configuring their servers to identify the location of the P3P policy. This will enable other P3P users to access the information.

P3P policies can be referenced in three different ways. It is expected that many server administrators will employ policy reference files in a well-known location to simplify web site administration. To do this, a policy reference file (p3p.xml) would need to be placed in a directory called /w3c, where /w3c is located under the root directory. A user agent could then request this file by using an HTTP GET request for the resource /w3c/p3p.xml. Alternatively, servers may be configured to insert a P3P header into an HTTP response to indicate the location of a site's P3P policy, or they can be configured to insert this information into HTML content as a LINK tag. More information about generating the policies/code for posting the P3P settings is available at http://p3ptoolbox.org/tools/resources1.shtml

4. How does P3P impact Web performance?

In most cases, the first time a user visits a Web site, their browser will have to make one or two additional requests in order to locate and fetch the P3P policy. These requests may impose some minimal latency; however, the delay caused by this should usually be less than the delay from fetching a single image in a Web page. Subsequent requests to the same site will usually not incur any additional latency due to P3P, as long as the site's policy has not expired.

5. Is P3P designed to replace cookie blocking software or anonymity tools?

No, P3P is complementary to cookie blocking software and anonymity tools. In fact, some of these tool vendors are building P3P into their products. P3P can offer users who want to selectively block cookies an opportunity to learn more about how each cookie will be used and direct their software to automatically block cookies that will be used for certain purposes while accepting cookies that will be used for other purposes. Anonymity tools are useful at sites where users have no reason to supply any personal information. However, when users wish to supply this information in order to complete a transaction, P3P is useful for informing users about how their data will be used. This is not a function performed by cookie blocking software or anonymity tools.

For more Info- http://p3ptoolbox.org/guide/

6. P3P User Agents in Action

Some organizations have released user tools that support P3P and others have announced plans to do so. The types of user agents that may emerge include Web browsers and plug-ins to Web browsers that provide different or additional P3P privacy features, media players, document readers, and software for wireless devices, such as personal digital assistants (PDAs) and Internet or e-commerce capable cellular phones.

The first user agents to emerge on the scene are Microsoft's Internet Explorer 6.0, a Web browser and AT&T Privacy Bird, a plug-in for Microsoft Internet Explorer 4.0, 5.0, 5.5 and 6.0. To get a sense of P3P in action here are descriptions of the offerings of Internet Explorer and the AT&T Privacy Bird:

Microsoft Internet Explorer 6.0

Microsoft has incorporated an implementation of P3P in its newest Web browser, Internet Explorer 6.0. At its most basic level, Internet Explorer 6.0 enables users to manage their privacy by giving them control over cookies based on the stated purpose of the cookie. This enables users to determine what Web sites they share information with and how those sites use that information.

Internet Explorer 6.0 does this by comparing the cookie´s machine-readable compact policy, with the user´s privacy settings. If the settings do not match or the cookie does not have a compact policy the cookie is either blocked or restricted. To alter user´s preferences in IE 6.0,

the user can change their privacy settings using the following privacy slide bar:

As with each user agent that is developed to work with P3P, Internet Explorer has its own set of rules for how to interact with P3P on the user´s behalf. Internet Explorer 6.0´s privacy controls are presented to users on a sliding scale of six settings in the Internet Options menu. The highest setting, Block All Cookies, denies all Web site requests for information using cookies regardless of privacy policy. The lowest setting, Accept All Cookies, allows Web sites to gather any information requested from the user using cookies. Microsoft also provides four intermediate settings, High, Medium High, Medium, and Low, which block or reduce the functionality and information uses of cookies based on a cookie´s P3P privacy policy.

Definitions: Cookie Actions in IE 6.0
Accepted: Cookie was accepted but might be leashed Restricted: Cookie was accepted but downgraded to a session cookie Blocked: Cookie was either suppressed or rejected

Definitions: Key Terms in IE 6.0 Privacy Settings
PII: Personally identifiable information, such as name, address, etc. **Non-Identifiable Information:** Data is seen as non-identifiable in the sense of the present P3P specification, if there is no reasonable way for the entity or a third party to attach the collected data to the identity of a natural person. **First Party Cookies:** Cookies that are placed on the user´s computer by the host domain of the Web site the user is visiting **Third Party Cookies:** Cookies placed on the user´s computer by any domain other than the host of the Web site the user is visiting **Persistent Cookies:** Cookies that are discarded when they reach their defined expiration time **Session Cookies:** Cookies that do not have a specific expiration time and are discarded when IE is closed **Downgraded Cookies:** A persistent cookie that is discarded when the session ends or at the expiration time, whichever is first **Leashed Cookies:** Cookies sent only on requests for first party content. When requests for third party content is made, these cookies are suppressed

Microsoft has set the Medium privacy level as the default when Internet Explorer is distributed. At this default setting, Microsoft has drawn a line to distinguish between satisfactory and unsatisfactory cookies. An unsatisfactory cookie contains or allows access to personally identifiable information that is used for unstated purposes or provided to recipients without user consent. (the Unsatisfactory Cookie Rule) This means that Internet Explorer 6.0 checks whether a compact policy´s purposes (e.g. IVD and OTP) and recipients (e.g. OTR) include opt-out or opt-in options for users (e.g. IVDo, OTPi, and OTRo).

The following chart summarizes the impact of IE 6 on cookies under the default user setting of Medium privacy.

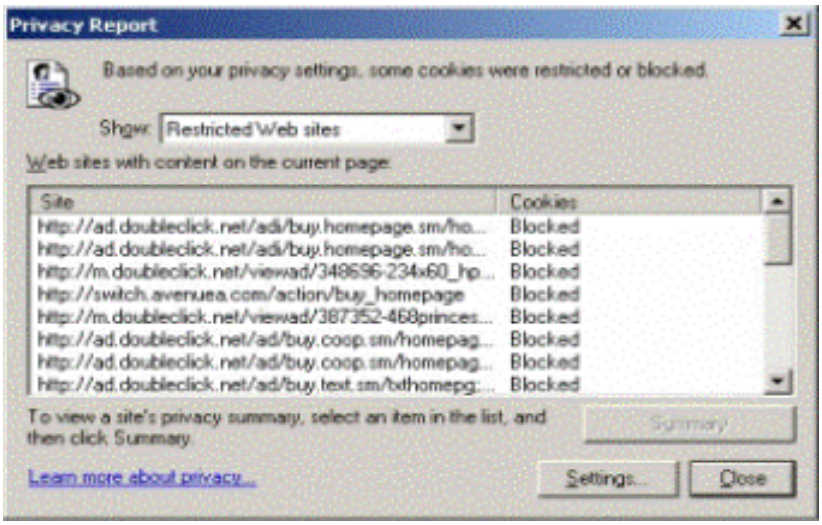
Cookie Type	Task	"Medium" Privacy setting	Implications for Compact Policy
First Party	Visited Web Site	If a first party cookie does not have a compact policy at all, then it will be restricted. If a first party cookie has a compact policy and the policy violates the unsatisfactory cookie rule, then it will be restricted.	a) If the site relies on the use of persistent cookies, then it should definitely deploy compact policies. b) If the organization offers users a way to opt-out of having their PII used for unstated purposes or disclosed to third parties, be sure to include os and Is as appropriate within the compact policy.
	User Experience	If a cookie has been restricted, a Web site will not be able to use information for Web ads, tracking, etc. once user leaves site.	

Cookie Type	Task	"Medium" Privacy setting	Implications for Compact Policy
Third Party	Visited Web Site	Blocks cookies without compact policies. Blocks cookies that ask for PII without user's implicit consent.	a) If the site relies on the use of third party cookies, then it should deploy compact policies with the third party cookies that it controls and require its third party vendors that set cookies to implement P3P compact policies as well. b) Third party cookies will be accepted only if one of the following is true: 1) The cookie collects or associates only non-identifiable information (represented by use of the NOI code within the compact policy); or 2) The cookie does collect or associate with PII but only after the user provides implicit consent, represented by attaching i to each purpose and recipient.
	User Experience	Any display or function requiring third party cookies that do not have compact policies will be blocked.	

In those cases that a cookie does not match the user´s privacy settings, the user will be notified by the privacy icon, which is an eyeball and a European do not enter sign icon (see below) in the browser´s bottom left icon tray. By clicking on this icon, users will be able to see what cookies were blocked, whether their sites have P3P privacy statements and, if so, what these statements are.

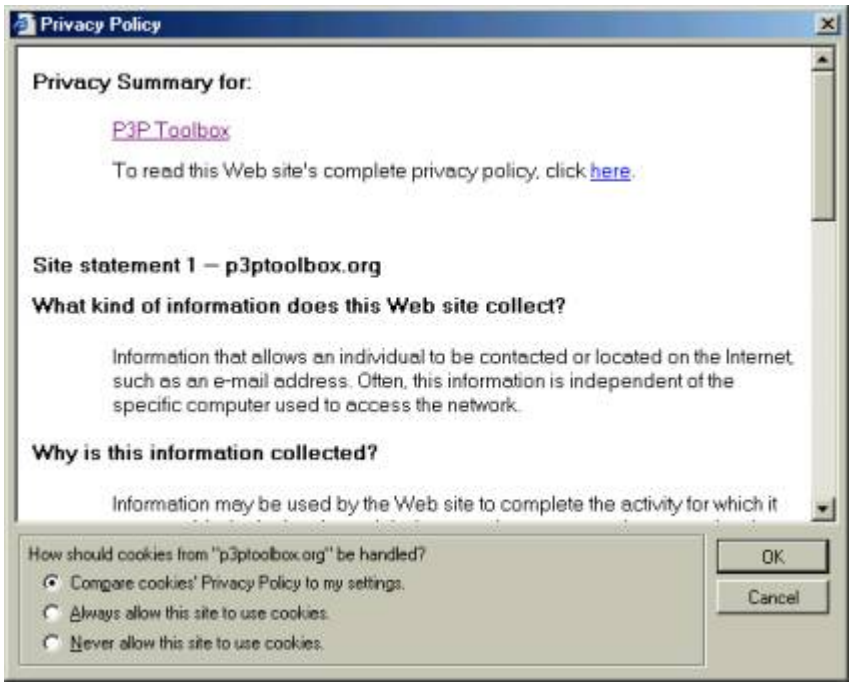
The Privacy Report

When the privacy icon appears, users will be able to click on it to view a Privacy Report,



which displays all of the graphics, charts and other date being sent by the Web site that the user is visiting and any third parties sending content from that Web site onto user´s computer. Depending on the user´s settings, the Privacy Report will display all Web sites setting information on the user´s computer or just the cookies or information that is being restricted because of the absence of a P3P compact policy or because the policy does not meet the user´s privacy settings. The user can than click on any cookie or other information being displayed in the report.

If the site has a P3P policy, the user will be able to view a human-readable P3P privacy summary that uses a common language and set of references for users to understand the privacy policies of the sites they visit. It will look something like this:



These summaries represent the human-readable summary of the machine-readable XML P3P policies. If the Web site does not have a P3P policy, the user will be directed to visit the site directly to read the Web site´s human readable privacy policy.
For a more detailed description of the Microsoft implementation of P3P, see Microsoft´s Internet Explorer developers´ Web site at http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnpriv/html/ie6privacyfeature.asp

AT&T Privacy Bird

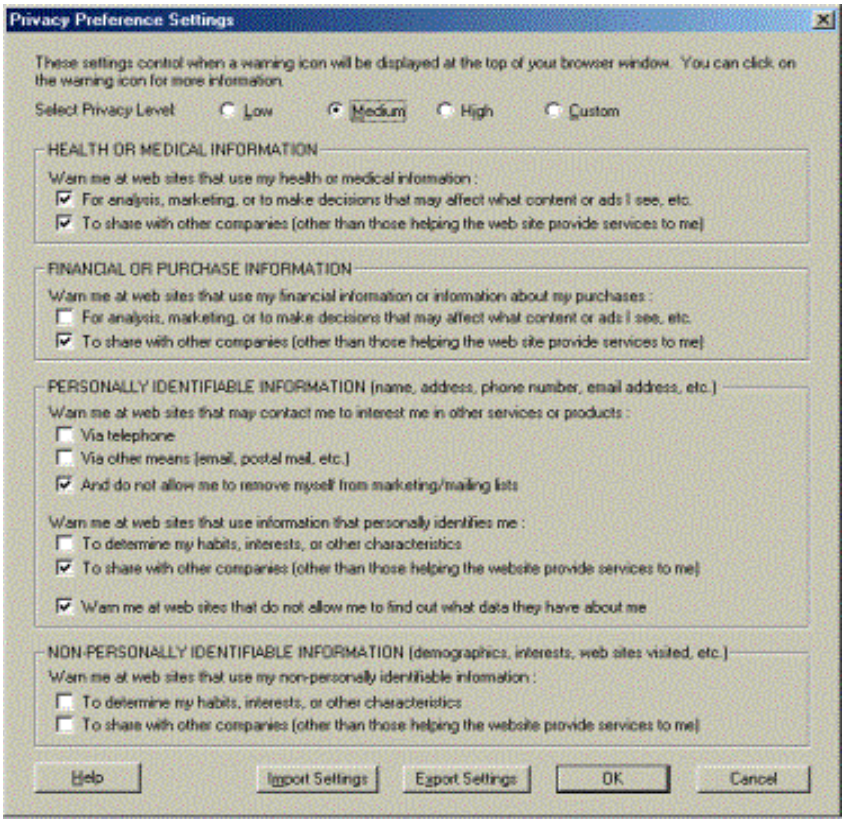
It is the first software to automatically read full P3P privacy policies and display them in an easy to understand language. It offers a wide variety of customization options, allowing you to tailor warning messages to meet your personal privacy concerns. For example, the AT&T Privacy Bird allows you to ask for warnings at Web sites that may:

- Sell your name and address to other companies without your permission
- Use your health or medical information for marketing
- Put you on mailing lists that you can't get off of

The AT&T Privacy Bird displays a bird icon in the top right of the user´s browser title bar and displays a different color of bird to indicate whether or not the Web site´s P3P policy matches the users preferences. The Privacy Tool can even be configured to provide an audible chirp to provide a warning.

Sample of title bar birds

The AT&T Privacy Bird provides a page for users to set their privacy setting preferences with the settings grouped into four categories: Health or Medical Information; Financial or Purchase Information; Personally Identifiable Information; and Non-Personally Identifiable Information. By checking the box next to a setting, the user controls which warnings to receive.



The AT&T Privacy Bird is a free download, available at http://www.privacybird.com/