Machine Readable Privacy Policy Guidelines

Last updated 9/10/2004

Act 1713 of 2003 requires state and local governments operating a website to incorporate a machine readable privacy policy into each of its websites no later than July 1, 2004. For this reason, the Office of Information Technology (OIT) has created these guidelines for agencies and counties to refer to when creating and maintaining machine readable privacy policies on their websites. OIT is in the process of promulgating an information technology standard that would require state agencies to use the P3P (Platform for Privacy Preferences) specification written by the World Wide Web Consortium (W3C). The P3P specification is the most common method of creating machine readable privacy policies today.

What is a "machine readable privacy policy"?

The World Wide Web Consortium, or W3C, describes P3P as:

"... a standardized set of multiple-choice questions, covering all the major aspects of a Website's privacy policies. Taken together, they present a clear snapshot of how a site handles personal information about its users. P3P-enabled Websites 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."

What is a "human readable privacy policy"?

A human readable privacy policy is a statement published in a traditional manner on a web page that details information its Website collects, with whom the data is shared, and how users can control the use of their personal data.

What are the requirements of Act 1713 of 2003?

You can read the actual language of Act 1713 of 2003 by going to:
http://www.arkleg.state.ar.us/ftproot/acts/2003/public/act1713.pdf

The act requires state and local governments to have incorporated a machine readable privacy policy into each of its websites by July 1, 2004.

Furthermore, the privacy policy statements must include:

1. A description of the data the agency collects on its website and how the data will be used by the agency
2. The type of data and the purposes for which data is shared with other entities
3. Whether the agency's data collecting and sharing practices are mandatory, or allow a browser to opt in or opt out of those practices, and
4. An explanation that certain information collected by the agency is subject to disclosure under the Arkansas Freedom of Information Act.

The act also requires agencies to create a link to, or instructions for, locating the website's policy reference file, which shall identify the uniform resource locator for the website's policy statement and shall indicate those portions of the website and the website's cookies that are covered by each statement.

Lastly, the act requires that agencies post a link to their human readable policy.

What is a "policy reference file"?

A policy reference file lists the P3P policies used by the site and states what parts of the site and what cookies are covered by each policy. A policy reference file can cover only resources on a specific host. Each host needs its own policy reference file. However, the policies themselves may be on another host.

What is a "compact policy"?

A "Full" P3P policy is a detailed XML document that fully describes all information collection practices for a site. In addition to Full Policies, sites are able to communicate their policies with regard to only cookie information through a mechanism called a Compact Policy. A Compact Policy is a custom HTTP header that is sent at the time a cookie is set. The Compact Policy, CP, uses a sequence of approximately 52 tokens to summarize a site's policy with regard to that cookie. Owing to compact policies' condensed nature they are far easier for web browsers to interpret and make decisions based upon than are Full Policies.

What is a cookie? How do cookies relate to this law?

A cookie is a message given to a web browser by a web server. The browser stores the message in a text file. The message is then sent back to the server each time the browser requests a page from the server. The main purpose of cookies is to identify users and possibly prepare customized web pages for them. When you enter a web site using cookies, you may be asked to fill out a form providing such information as your name and interests. This information is packaged into a cookie and sent to your Web browser which stores it for later use. The next time you go to the same Web site, your browser will send the cookie to the Web server. The server can use this information to present you with custom Web pages. For example, instead of seeing just a generic welcome page you might see a welcome page personalized with your name.

Do I have to put a machine readable privacy policy on each page of my website?

When deploying P3P, the website developer can choose how many policy statements to use to cover the site. This consideration may seem strange for someone accustomed to text-based privacy policies, but there is an important distinction for P3P privacy statements. A P3P privacy statement is specific about the data or types of data being collected by the site. Thus the statement will list specific elements of data that the site collects, such as "User's name", or else specific types of data which the site collects such as "User's physical contact information".

This is important as websites generally collect different amounts of data in different parts of the site. For example, a website may collect no information about the visitor's name and address at the site homepage, but may need detailed contact information to complete an order.

In the P3P protocol it is acceptable to publish a statement which overstates the data collection of the site. Thus it's allowed to have a single policy which covers all of the data collected anywhere on the site. However, it is in the site's interest to have more specific P3P statements. In the example above, the site doesn't need to claim - and probably doesn't want to claim - that it needs the visitor's name and address just to access the homepage when that information is really only needed to submit an order. This could scare away visitors who are simply browsing.

It's also in the site's interest to use as few P3P statements as possible to cover the site. After all, it takes time to create a P3P statement, and managing 100 P3P statements on a single site is probably unrealistic even for the most heroic webmaster. Thus, a site needs to strike a balance between specificity and number of policies. While there is no right answer for every site, most sites can be covered by five or fewer P3P statements, and it is a very rare site which needs more than 10 P3P statements.

Where can I learn how to use the P3P specification?

There are many good places to learn how to use the P3P specification. Here are a few:

The Platform for Privacy Preferences 1.0 Deployment Guide:
http://www.w3.org/TR/2001/NOTE-p3pdeployment-20010510#How_Many_Policies

Platform for Privacy Preferences (P3P) Project:
http://www.w3.org/P3P/

P3P Toolbox:
http://www.p3ptoolbox.org/

Where do I get help in becoming compliant with Act 1713?

If your site is hosted by the Information Network of Arkansas, you may contact them at info@ark.org, or you may call INA at 501-324-8900 or 1-877-727-3468. You may also contact the Technology Investigation Center at tic@arkansas.gov or by calling 501-682-4307.

My website is hosted by the Information Network of Arkansas (INA). Are they writing my privacy policy?

INA has implemented three privacy policies that can cover most of the websites of their hosted clients. These policies are general in nature. They describe the following website practices:

1. Web stats only policy - for use on sites that log web server statistics only and are informational sites.
2. Data collection policy - for use on sites that collect data from users for surveys, simple forms input, requesting an item to be mailed, etc.
3. Payment collection policy - for use on sites that collect data as above and in addition, purchasing or payment data.

Although INA has posted these three policies, each agency must be responsible for determining the appropriateness of these policies for their agency website practices. Furthermore, each agency must go to the agency toolkit form here: https://www.ark.org/toolkit/privacy_policy/index.php In the form agencies must indicate their acceptance of the existing INA policies or provide their own privacy policies. INA will work with agencies they host if they need custom policies to make their websites compliant.

How do I get started writing my human readable privacy policy?

First, look at the legislation. It has six components:

The privacy policy statements must include:

- A description of the data the agency collects on its website and how the data will be used by the agency
- The type of data collected and the purposes for which this data is shared with other entities
- Whether the agency's data collecting and sharing practices are mandatory, or allow a browser to opt in or opt out of those practices, and
- An explanation that certain information collected by the agency is subject to disclosure under the Arkansas Freedom of Information Act.

The act also requires agencies to create a link to, or instructions for, locating the website's policy reference file, which shall identify the uniform resource locator for the website's policy statement and shall indicate those portions of the website and the website's cookies that are covered by each statement.

Lastly, the act requires that agencies post a link to their human readable policy.

Requirement 1:

- A description of the data the agency collects on its website and how the data will be used by the agency

There can be many types of information collected by a website. The following paragraphs describe types of information that your agency website may gather.

Personal Information

"Personal Information" means any information related to a person, which includes their name, number, symbol, mark or other identification that represents that person. We do not and/or are not obligated to gather any information about you unless you provide that information voluntarily through an e-mail, response through a survey or completing an on-line transaction.

We automatically collect and archive the following information: User hostname, HTTP header (user agent), HTTP header (referrer), System Date, Full Request, Status, Content Length, Method and

Universal Resource Identifier. The information that is collected is automatically used to improve the website's content and to help us understand what our users needs are. This information is collected for statistical analysis, to determine what information is of most and least important and to improve our marketing purposes.

Cookies Usage

We also use cookies (text files stored on your web browser to provide a means of distinguishing among users of the website). Cookies are used for the purposes of tracking information purposes only, but do not contain any ***personal information*** about the viewers.

Information Collected through E-mail

Your e-mail address and the contents of your message will be collected. The information collected is not limited to text characters and may include audio, video and graphic information formats included in the message. Your e-mail address and the information included in your message will be used to respond to you, to address issues you identify, to improve this website, or to forward your message to another state agency, coalition, organization or group (all depending on your needs) for appropriate action. The viewers e-mail address is not collected for commercial purposes and we are not authorized to sell or otherwise disclose your e-mail address for commercial purposes.

Transactions Completed

If the viewer completes a transaction, such as a survey, registration form or order form, the information, volunteered by you, will be used by the agency.

Logging

This agency uses login events when the viewer registers on this site. The collected information is the user registration, the time of user logon and the time of user removal from the system. If the user posts anything on our site, the information will be archived.
This agency does not knowingly collect personal information from children or create profiles on children. Users are cautioned, however, that the collection of personal information submitted in an e-mail will be treated as though it was submitted by an adult, unless exempted from access by federal or state law, and be subject to public access. We strongly encourage parents and teachers to be involved in their children's or students activity on the internet.

Example of privacy policy verbiage that your organization might use if you collect information from users on your website:

Our agency collects your name and address in order to send you monthly newsletters.

Example if your organization doesn't collect data from the users, but your organization runs programs in the background that monitor visitors.

The IP (Internet Protocol) numbers of computers used to visit [network] sites are noted as part of our statistical analysis on use of our web sites and how to better design services and facilitate access to them.

Requirement 2

- The type of data and the purposes for which data is shared with other entities

Example of privacy policy verbiage that your organization might use if you collect information from users on your website and share the information:

Our organization shares the information we collect from you with <federal agency name> in order to provide you with our agency services. The federal agency requires that we submit a list of those receiving our agency services to be reimbursed for the cost of providing those services.

Example of privacy policy verbiage that your organization might use if you collect information from users on your website and don't share the information:

Our agency does not share data you provide us with any other entity.

Requirement 3

- Whether the agency's data collecting and sharing practices are mandatory, or allow a browser to opt in or opt out of those practices, and

Example of privacy policy verbiage to address mandatory data collection:

Our agency collects server log files, uses WebTrends or other site analysis software that uses code to collect usage information, or logging done by applications accessed by your website. This collection process is mandatory and visitors to our site are not allowed to opt out of this data collection mechanism.

Example of privacy policy verbiage that allows users to opt in:

You may opt in to share your mailing address with other Arkansas agencies and receive brochures about Arkansas tourism by checking the box on the web page where you enter your mailing address.

Example of privacy policy verbiage that allows users to opt out:

The Department of Health will use information we collect to contact you about other state services you may be eligible for. If you don't want us to share your personal information with other agencies, you may opt out by checking the opt out box on the web page where you enter your personal information.

Requirement 4

- An explanation that certain information collected by the agency is subject to disclosure under the Arkansas Freedom of Information Act.

Example of privacy policy verbiage referring to the Freedom of Information Act:

The information collected on this website is subject to the same controls and uses as that collected by governmental offices visited in person, subject to the access and confidentiality provisions of the Arkansas Freedom of Information Act, Ark Code Ann., §§ 25-19-101 through 25-19-107, or to other applicable sections of the Arkansas Code.

The act also requires agencies to create a link to, or instructions for, locating the website's policy reference file, which shall identify the uniform resource locator for the website's policy statement and shall indicate those portions of the website and the website's cookies that are covered by each statement. Lastly, the act requires that agencies post a link to their human readable policy.

The policy reference file, which gives the URL for the site's policy statements and indicates what portions of the site and which of the site's cookies are covered by P3P statements, is an XML document that is typically a few kilobytes in size. The policy reference file must be published on the web site.

P3P policies and policy reference files always use the same syntax, but there are three different ways by which Web clients can locate the policy reference file for a page:

- Place the policy reference file in the "customary location" (at /w3c/p3p.xml on the site).
- Add an extra HTTP header to each response from the Web site that gives the location of the policy reference file.
- Place a link to the policy reference file in each HTML page on the site.

Now that I have my human readable policy done, how do I create a machine readable privacy policy?

Here are some available tools you can use:

AlphaWorks – IBM P3P builder
http://www.alphaworks.ibm.com/formula/p3p
http://java.sun.com/products/archive/j2se/1.3.1_09/

HiSoftware – P3P Policy Builder
http://www.hisoftware.com/downloads/p3pbuilder.exe

EZP3P – P3P XML Utility
http://downloads-zdnet.com.com/3000-2068_2-10198118.html

P3P Edit – Web based utility
http://p3pedit.com/

Each of these utilities has separate advantages ranging from ease of user interface to in-depth ability to create complex P3P policies.

Factoring the following to make recommendations:
Ease of use with a rating of 5 being the easiest to 1 being the most complex (learning curve)
Cost with a rating of 1 being free to 0 indicating fees associated with product
Scalability (compact/complex) with a rating of 5 being the most versatile to 1 being non-modifiable

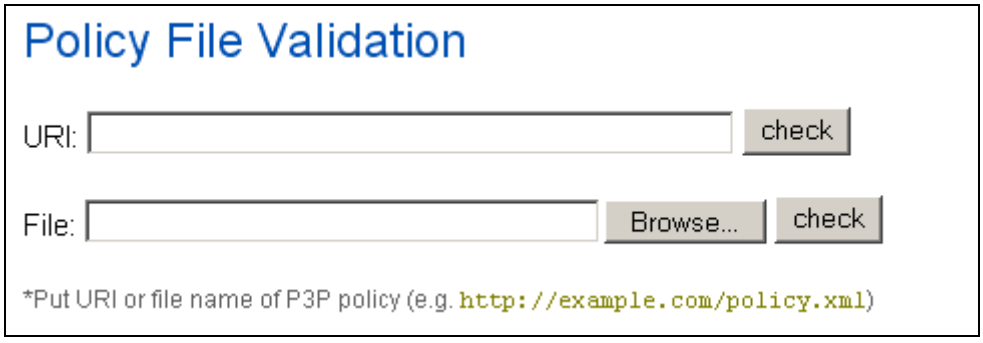
Utility / Software	Cost Rating (0-1)	Ease of use (5-1)	Scalable (5-1)	Overall
HiSoftware	Free (1)	4	3	8
AlphaWorks	Free (1)	1	5	7
EZP3P	Free (1)	3	2	6
P3P Edit	49.00 (0)	2	1	3

How do I validate my P3P policy?

The World Wide Web Consortium (W3C) has provided a way to evaluate the syntax of the policy and all the machine readable files working together. This P3P testing is available at the following URL:
http://www.w3.org/P3P/validator.html

Documentation for this product is available at http://www.w3.org/P3P/validator/20020128/document

To test the machine readable policy file, either enter the URI (uniform resource identifier) if the file has been posted on the Internet or enter the file's name. You may browse to find the file on your network.



Then click on the appropriate check button. Here is an example of a successful Policy validation:

Results of P3P Policy validation

Target URI: http://www.hud.gov/w3c/hud.xml

Step 1: **Policy File Validation**

URI: http://www.hud.gov/w3c/hud.xml

Step 1-1: Syntax check

Policy file has no syntax errors.

Step 1-2: Vocabulary check

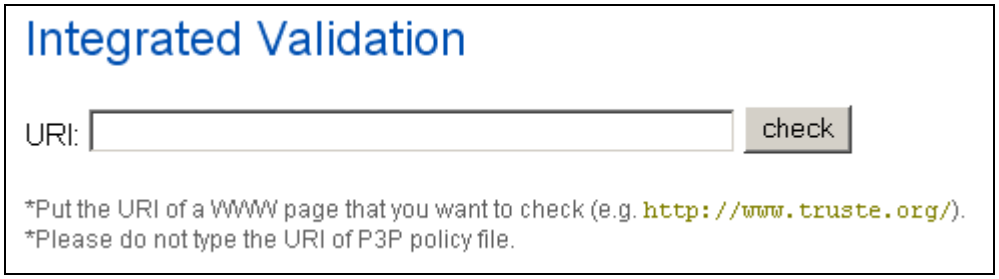
Policy file has no vocabulary errors.

Step 1-3: Link check

Policy file has no link errors.

Message: line 8: discuri attribute of <POLICY> element can be accessed.

To test the Machine Readable P3P on the website, first make sure and upload the P3P files to the appropriate location. Then, enter the URI of any web page that you want to test. You may want to test your website home page first.



Then click on the appropriate check button. Here is an example of a successful P3P validation:
Results of P3P Policy validation

Target URI: http://www.hud.gov/

Step 1: **/w3c/p3p.xml Validation**

URI: http://www.hud.gov/w3c/p3p.xml

Step 1-1: Access check

/w3c/p3p.xml can be retrieved.

Message: The content type of /w3c/p3p.xml is **text/plain**.

Step 1-2: Syntax check

/w3c/p3p.xml has no syntax errors.

Step 1-3: Policy URI check

/w3c/p3p.xml has no warnings or errors.

Message: P3P policy indicated at line 4 can be accessed.

P3P policy for http://www.hud.gov/ is [http://www.hud.gov/w3c/hud.xml#hud]

Step 2: **HTTP Protocol Validation** (HTTP headers)

HTTP headers have no P3P: header.

Step 3: **HTML File Validation**

HTML document has no P3P compliant link tags.

Message: No valid P3P compliant `<link>` element.

Step 4: **Policy File Validation**

URI: `http://www.hud.gov/w3c/hud.xml#hud`

Step 4-1: Syntax check

Policy file has no syntax errors.

Step 4-2: Vocabulary check

Policy file has no vocabulary errors.

Step 4-3: Link check

Policy file has no link errors.

Message: line 8: `discuri` attribute of `<POLICY>` element can be accessed.

Here is an example of a website with errors in its P3P files.

Results of P3P Policy validation

Target URI: `http://www.arkansas.gov/`

Step 1: **/w3c/p3p.xml Validation**

URI: `http://www.arkansas.gov/w3c/p3p.xml`

Step 1-1: Access check

/w3c/p3p.xml can be retrieved.

Message: The content type of `/w3c/p3p.xml` is **text/html**.

Step 1-2: Syntax check

`/w3c/p3p.xml` is NOT an well-formed XML file.

```
not well-formed (invalid token) at line 85, column 17, byte 2150:
<script LANGUAGE="JavaScript1.2"> var version = 1.2;</script>
<script LANGUAGE="JavaScript1.3"> var version = 1.3;</script>
<script language=javascript>
================^
function add_favorite(favlink, linktype){

     window.open('../add_favorite.php?link='+favlink+'&type='+linktype+'
&PHPSESSID=',"login","toolbar=no,scrollbars=no,width=200,height=250,menu
bar=no");
```

Step 2: **HTTP Protocol Validation** (HTTP headers)

HTTP headers have no `P3P:` header.

Step 3: **HTML File Validation**

HTML document has no P3P compliant link tags.

Message: No valid P3P compliant `<link>` element.

Validator could not find valid policy reference file URI. Validation aborted.

How do I maintain my privacy policy?

The Validator will check for correct syntax and file location, but cannot compare actual privacy practices to the statements made in machine or human readable privacy policies. Manual review is the only way to assure that machine readable and human readable policies are kept synchronized and accurately describe the practices of the website. Every time a website's machine readable privacy policy is updated it should be re-validated. Periodic review should include consideration of the following:

- Changes to the website that involve the collection or use of data
- Changes to the website that indicate visitors to your website should refresh their caching of your machine readable privacy policy more or less frequently
- Changes to the P3P Specification

Sources for Machine Readable Privacy Policy Guidelines: Webopedia, The Platform for Privacy Preferences 1.0 Deployment Guide, Platform for Privacy Preferences (P3P) Project, submissions from Privacy Working Group members