

BITS

FINANCIAL SERVICES
R O U N D T A B L E

NOTE: This letter has been submitted electronically to www-p3p-public-comments@w3.org.

October 15, 2001

Dear Members of W3C and the P3P Working Group:

Introduction

The following comments on the Platform for Privacy Preferences 1.0 (P3P 1.0) Specification, W3C Working Draft of 24 September 2001, are submitted by BITS, The Technology Group for The Financial Services Roundtable. Membership in BITS and the Roundtable is reserved for the 100 largest integrated financial services companies in the United States. BITS works directly with the CEOs, CIOs, CTOs, and heads of technology, privacy, e-commerce and security-related areas within these major financial institutions. BITS serves the financial services industry at the interface of commerce, technology and financial services. Our major areas of focus are standards, privacy, security, e-commerce market development and leveraging the infrastructure of the financial services industry. BITS' mandate includes facilitating the growth of electronic commerce; facilitating development of superior, market-driven technologies; and sustaining consumer confidence and trust by ensuring the safety, soundness, privacy and security of financial transactions. With this mandate in mind, our members believe it appropriate for us to submit these comments for consideration. They are submitted on October 15 in order to accommodate the review schedule presented by W3C. BITS and our members will further vet these recommendations and will submit revised suggestions for W3C's consideration, should that be warranted. We appreciate the opportunity to comment.

High-Level Comments and Recommendations

- It would be accurate and appropriate for the W3C to state explicitly that P3P is neither a legal nor an audit standard and should not be treated as such in contracts, site monitoring, and for other legal and regulatory purposes.
- We encourage a roll-out strategy that reflects the view that development and implementation of P3P is an evolutionary process, at an early stage. Therefore, certain elements included in the first stage should not lead to disproportionate negative impacts.
- We request that W3C work with the financial services industry to make changes in the language of P3P. P3P has been developed to intentionally limit the ways in which an

entity can express its privacy policy; for example, one of the most significant decisions of the P3P Working Group was not to enable use of the word “may” within the P3P nomenclature. We believe that the P3P nomenclature should enable verbatim translation of existing plain language policies, and that failure to incorporate that capability will materially affect the speed with which this standard is adopted in the marketplace. Although such a fully robust specification may not be possible in Version 1.0, key omissions, such as the word “may” noted above, should be corrected in the final version of the current generation. The current P3P language cannot handle the complex requirements of the European Union Directive, Gramm-Leach-Bliley, HIPPA, COPPA, or other specific laws and regulations. For example, real world cookie statements at a corporate level often include the word "may." The actual usage is then made explicit for the particular page or service where a cookie is used.

- We recommend that a means be specified whereby the User Agent (e.g. browser) can communicate back to the service when it is actually blocking or downgrading a request (e.g., blocking or downgrading a cookie).
- The compact policy section is listed as optional. Considering that the first implementation requires and only looks at compact policies, and that this was based upon difficulties in implementing the full specification within accepted performance constraints, it is recommended that the compact policy should be changed from “optional” to “required.” If this is not the desire of the W3C, then User Agents should be required to follow the specified practices now recommended.
- A service should be able to declare domains that are actually part of the same organization and should be treated as first parties. This should be possible by pointing to a file that lists those domains that actually are part of the same organization and should be treated as first party cookies, and/or listing those domains in the compact policy (that is adding tokens to the compact policy that indicates those URI’s whose domains should all be treated as first party cookies). While the HINT method may work for site policies, no such tool is available at the compact policy level.
- It should be made clear that "compact policies" should only address cookie practices and these may or may not reflect the overall use of information on the site.
- It should also be made clear that P3P policies should only address the information gathering and use practices on specific sites, pages, and services and should not be interpreted as a company's overall privacy policy.

Organization of Detailed Comments

The following detailed comments address four major topics:

- Legal and Regulatory Environment
- Extension of Language for Organizations and Services Now Impacted by P3P
- Clarification of Terms and Intent
- Additional Suggestions

Legal and Regulatory Environment

Current deployments of User Agents have the potential for significant legal risks to the web community, whether or not the particular site implements P3P policies. This comes from a misunderstanding of where P3P is in the development cycle:

- Requirements for compliant P3P language are now being asked for in contracts.
- There is a stated intention of regulators to compare P3P language to actual behavior.
- There are potential conflicts between how a P3P implementation characterizes site behavior and a company's own plain language privacy policy, which could appear to lead to charges of bad faith.

Therefore, the next release of the specification should clarify that this current specification is not meant as a legal or audit document. It should also say that there is likely to be a significant amount of testing and development required at this phase of the process. This would allow sites to comfortably say that their P3P statements and compact policies are not meant to be legally binding documents and may simply be the only settings that allow certain sites to work. While this has been a recommended strategy by some legal experts, regulated sites would be better served if this were made part of the current specification. If sites choose this approach, they should direct users to their plain language policy and tell them that P3P implementation will evolve as the technology becomes available.

Specific requested changes to reduce legal risk include:

Add a paragraph to "Status of Document" (before current last paragraph) to read:

While W3C members understand the maturity of specifications at different points of development, the outside world is treating current P3P implementations as the well-tested outcome of a mature specification.

Add a paragraph at the end of "1. Introduction" to read:

Since it is impossible for a browser to understand whether a site, page, or object should have a privacy policy, this version introduces "and compact policy tokens for: purely commercial sites, pictures, certificates, clear gifs for anonymous counts, and other pages that have cookie like behavior but which do not capture or use personally identifiable information."

Add three paragraphs before the current final paragraph in 1.1.3 to read:

At this time, the language of P3P may not be adequate to express all of the elements required in certain legal notices, such as the U.S. Gramm-Leach-Bliley Act and FCRA in financial services, HIPPA, COPPA, the European Union Data Protection Directive, and other sector-specific practices. The language is still limited in terms of its ability to express the nuances that are becoming part of plain language notices. There is not yet a framework for sites that may be picked up by browsers as sites or pages that should have a notice, but which are pictures, certificates, counters, purely

B2B sites, or otherwise not covered by privacy laws, regulations, or self-regulatory requirements.

There is also extended legal liability for having notices that are not legally accurate. For example, the FTC in the U.S. has the ability to prosecute site owners for having inaccurate notices. Therefore, it may be appropriate for sites implementing P3P1.0 to have a statement that disavows legal or moral significance to compact policy tokens where available tokens cannot adequately express the working of the site. For example, current implementations capture company sites as being "third party sites." In addition, "dummy tokens" may be necessary for B2B sites, certificates, pictures hosted on other servers, and other practices which do not involve "cookies" or "personally identifiable" information.

Agencies with the responsibility for enforcing privacy policies should understand that the current implementation of the P3P1.0 specification should be seen as a very large scale test of the ability of P3P to accurately reflect real world privacy policies and statements. There may still be a number of problems with both the language and with particular implementations. Therefore, legal liability should be postponed until the lessons from this test have been incorporated into a final version.

Add a paragraph at the end of 1.1.4 to read:

At the current time, P3P User Agents are in the initial stages of implementation. These may not incorporate the full P3P specification. Limitations of "machine to machine" communication may behave somewhat differently than policy developers had expected. Despite these limitations, companies have been encouraged to make such agents available so that P3P policies can be tested and used. Details of these specific implementations, where different from the P3P specification, should not be seen as indications of how P3P agents should be developed in the future. Future releases should correct or counterbalance these short-term limitations.

Important policy statements are buried in later sections. These may lead to the current misinformation about P3P, such as that it will encode a company's current privacy policy. This document should clearly define these to be outside of the scope, at least for now.

For example, Section 2.3.5 on the Access element says: "...the scope of P3P statements is limited to data collected through HTTP or other Web transport protocols. Also, if access is provided through the Web, use of strong authentication and security mechanisms for such access is recommended; however, security issues are outside the scope of this document."

The introductory section should clearly say that information collected off-line is not and should not be covered in a P3P statement at this time. This may be possible in later phases.

The introductory section should also clearly say that security mechanisms, and other significant privacy issues, are also not now covered in the P3P language but may be in future versions.

Section 3.3.5 'The RECIPIENT' element should be included to provide for additional "exemptions" where sharing does not need to be covered so that P3P statements can focus on meaningful differences. For example, the list of Gramm-Leach-Bliley exceptions may be a good place to start. These may also be covered in the introduction as items that should be in the human readable policy and which are not provided for in the P3P elements.

For example, there should also be other standard exceptions:

- When other required disclosures are provided when certain information is captured with customers' permission or at their direction. For example, required disclosures for sending data to credit bureaus are very explicit.
- Transfer of data on sale [or bankruptcy] including use of the data for due diligence before the sale. This would be covered in the overall corporate privacy policy and should mean information captured on-line as well as off.
- Access via legally served court order, regulation, or other legal process.
- Access for fraud control, security, or continuity of business vendors.
- Access for staff who maintain website under the control of the business.
- Potential access by others who own or operate the computer terminal and site where the user accesses the site—through caching, click stream capture programs, employee monitoring programs, or other methods.
- Etc. (See GLB for banking examples. Others occur in HIPPA, Freedom of Information Act, and other legal documents.)

Extension of Language for Organizations and Services Now Impacted by P3P

Many sites and services will be impacted by Browsers with Default P3P preferences turned on. This is true even for sites that do not work with consumers or consumer data. There are also many services that may appear to have cookie-like behavior but which are used for other purposes.

Therefore, site developers should have elements and tokens to identify sites and services that should not be impacted by P3P or other privacy policies. Ideally, these would:

- Have a brief policy with only one or two required statements; or
- Have a single "token" in the Compact Policy.

Worst case, these could be described in the same section (3.3.3) as 'The NON-IDENTIFIABLE' element. However, this would still require a significant number of statements. For the compact policies, these may all share the same "NOI" token, even though these may cover areas as diverse as:

- Purely corporate sites.
- Business to Business sites.
- Pictures or other materials (PDF files) hosted on a different server.

- Certificates
- Purely "counting" devices with only non-identifiable information.
- [This is not meant to be a complete list at this time. The list will need to be expanded as current implementation programs identify additional situations.]

Clarification of Terms and Intent

There is need for additional clarity about how P3P is supposed to work, since the current requirement still contains much ambiguity and many items are suggested but not developed or resolved.

It would be helpful to have one chart or section which could say:

- Names of each element;
- Whether this element is required (and whether this may be required if other optional elements are or are not used);
- Default (and consequences) if this element is not included; [often buried] and
- Whether or not it applies to cookies or just to sites.

In 1.3 Definitions:

Change "**Identified Data**" to "**Personally Identifiable Data (PI)**" to better match other Internet privacy usage.

The definition for **Repository** is limited to user information stored under the control of the user agent. However, in 5.6.4. it is also used to define data stored under the control of the service provider. While the User Agent Repositories are an extremely important subject for both browsers and P3P, it is not adequately covered in this specification. We recommend either tackling it in the next phase or leaving it out.

The concept of **Safe Zone** is similarly abstract and may be more appropriate for the next phase.

The terms "**Site**", "**Service**" and "**Page**" are not used carefully or consistently throughout the document. For example, while most compact policies appear to be handled at the "Service" level, all references are to the "Site." This may be easier to incorporate consistently if there were a defined term for a "**P3P Impacted Service**." This may be one that included one or more cookie behaviors. Note that Service is currently defined as: A program that issues policies and (possibly) data requests. By

this definition, a service may be a server (site), a local application, a piece of locally active code, such as an ActiveX control or Java applet, or even another User Agent.

While this specification recognizes the concept of **Service Provider (Data Controller, Legal Entity)**, with an appropriate definition, this concept appears to have been lost in the actual implementations, where there is little difference between a third party web site under the control of the Service Provider and a third party web site which is not under that control. Future specifications should work to implement technologies so that a third party web site under the control of the Data Controller is treated as such. There must be a better way, outside of hard coding each element, to capture and use this.

Since **Statement** is a very important concept, the definition should be expanded to show the scope. For example, this could read: "A P3P statement is a set of privacy practice disclosures relevant to a site, page, or other Service, such as a server (site), a local application, a piece of locally active code, such as an ActiveX control or Java applet, or even another User Agent. This talks to the collection of data elements on that service."

The definition of **User** should be expanded to indicate impact on how data should be classified. : For example: An individual (or group of individuals acting as a single entity) on whose behalf a service is accessed. P3P statements address the capture and use of personal data about this individual or group.

The definition for **User Agent** should clearly point out that this is only software. While pointing out how it SHOULD work, there also should be some cautions to indicate that it may not always work in that way. For example, anyone sharing a machine with this User Agent installed, such as another family member, an employer, a public institution (library/school) may not be allowed to change the set preferences. . [There appears to be also an intent to say here that the service is not allowed to change the settings without notifying the user. If this is the desire, this should be said outside of the definitions section.]...."

The last paragraph of 2.2 raises many ambiguities. These are also raised, but not resolved, throughout the document.

This now says: "This document does not specify how P3P policies may be associated with documents retrieved by means other than HTTP. However, it does not preclude future development of mechanisms for associating P3P policies with documents retrieved over other protocols. Furthermore, additional methods of associating P3P policies with documents retrieved using HTTP may be developed in the future. "

While this may be true, it leaves the user hanging. Will this be resolved by the time the standard is finalized? Should User Agents bypass such documents? For example, it is unlikely that a PDF file would either be setting cookies or have a P3P statement. This at least would allow for certainty in implementation. It is not

desirable to allow each User Agent to define whatever rules they want, leading to sites that will function differently with different browser implementations.

Section 2.3.2.3.3 "Requesting Policies and Policy Reference Files" raises a problem where there may be HTTP 1.0 caches.

The proposed solution provides a very difficult scenario for developers, who would theoretically need to know if any user cache site were still using HTTP 1.0 and implementing around this. This would be much simpler if the User Agent developer were told to refresh the policy if an HTTP 1.0 cache were encountered.

Paragraphs in Section 2.3.4 provide a significant amount of ambiguity by having loose requirements for User Agents which lead to the suggestion that services should implement many defensive measures which may or may not actually work. Recommendation: Leave things that are this complex to the next phase, giving service providers some latitude, especially with the limitations of current User Agents to handle complexity. For example, the second paragraph reads:

If a User Agent is unable to find a matching include-rule for a given *action URI* in the policy reference file that was referenced from the page, it SHOULD assume that *no* policy is in effect. Under these circumstances, User Agents SHOULD check the well-known location on the host of the action URI to attempt to find a policy reference file that covers the action URI. If this does not provide a P3P policy to cover the action URI, then a user agent MAY try to retrieve the policy reference file by using the HINT mechanism on the action URI, and/or by issuing a HEAD request to the action URI before actually submitting any data in order to find the policy in effect. Services SHOULD ensure that server-side applications can properly respond to such HEAD requests and return the corresponding policy reference link in the headers. In case the underlying application does not understand the HEAD request and *no* policy has been pre-declared for the action URI in question, user agents MUST assume that *no* policy is in effect and SHOULD inform the user about this or take the corresponding actions according to the user's preferences.

For the same reason, the "SHOULD NOT" in the following paragraph should be changed to a "MUST NOT":

Note that services might want to make use of the <METHOD> element in order to declare policies for server-side applications that only cover a subset of supported methods, e.g., POST or GET. Under such circumstances, it is acceptable that the application in question only supports the methods given in the policy reference file (i.e., HEAD requests need not be supported). User agents SHOULD NOT attempt to issue a HEAD request to an action URI if the relevant methods specified in the form's method attribute have been properly pre-declared in the page's policy reference file.

Section 2.5 provides several examples. If a particular User Agent (such as IE 6.0) does not behave in this way and it affects the performance or requirements at a Service site, who has

the responsibility of telling developers what to do to be in compliance? For example, Example 1 does not appear to require compact statements for cookies to be correctly handled. Current language reads:

Scenario 1: Web site basic.example.com uses a variety of images, all of which it hosts. It also includes some forms, which are all submitted directly to the site. This site can declare a single P3P policy for the entire site (or if different privacy policies apply to different parts of the site, it can declare multiple P3P policies). As long as all of the images and form action URIs are in directories covered by the site's P3P policy, User Agents will automatically recognize the images and forms as covered by the site's policy

Section 3.2.2. on the Policy element could be clearer about what the referenced page from **opturi** should or must contain, since the act of opting-in may be an integrated part of signing up for a service. For example, many opt-in programs simply tell the user (on each page that collects information) to only input information if they want information to be used. There is no point in collecting information and then marking it so that it cannot be used. Therefore, there may not be a single URI for this. For example, a second sentence could be added so the description would read:

URI of instructions that users can follow to request or decline to have their data used for a particular purpose (opt-in or opt-out). This attribute is *mandatory* for policies that contain a purpose with required attribute set to opt-in or opt-out. This can be a generic description of how opt-ins and opt-outs are handled and does not need to be a specific page from which all opt-ins or opt-outs for a company may be managed.

Section 3.2.3 could better explain the purpose of the **TEST** element. Current description simply says that it will cause a policy to be ignored. Is there actually a way to test a site's performance using a policy with a TEST element?

Section 3.2.5 on the **Access** element appears to be very helpful in terms of data which are addressed. However, there are internal inconsistencies:

When used in a Compact Policy, this would imply that the compact policy would only need to get access to data carried on cookies. For most companies, this would be "No Personal Information." However, policy enforcement agencies, like the US Federal Trade Commission, may not come to the same reading going through this specification.

The second paragraph clearly says: "However, the scope of P3P statements are limited to data collected through HTTP or other Web transport protocols." [This does not appear to be a consistent point of view throughout the specification.]

Also, if access is provided through the Web, use of strong authentication and security mechanisms for such access is recommended; however, security issues are outside the scope of this document. [Are these intended for future documents?]

Also in 3.2.5 and in many other sections "sites" is used instead of "service." (The discussion for **<nonident/>**):

While the elements are the same for both "sites" and "services which use cookies," having a single description that applies to both types of uses introduces a great amount of confusion. Either there should be a second section which discusses these elements when used in a cookie statement, or each of the descriptions should separately state how these work for sites and how they work for services that employ cookies.

Also in 3.2.5, the description under **<contact-and-other/>** should be made simpler and clearer.

Simply say that this would result in the same behavior as saying both **<ident-contact>** and **<other-ident>**.

In the overview for Section 3.0, or specifically in 3.3 The NON-IDENTIFIABLE element, it should be made clear whether any of the other Statement elements are required if this option is selected. In fact, most do not make sense if no identifiable information is captured.

For example, it would seem as if a statement with NON-IDENTIFIABLE would not need PURPOSE, etc. This is never clearly stated.

This section also appears to be a logical place to identify other sites and services that should not be impacted by P3P policies, since these would go significantly beyond any law or even self-regulatory program. See above.

In 3.3.6, the **Retention** element, many sections, such as **<legal-requirement/>** impose significant requirements on sites. If these are important, they should be raised to the top.

For example, there is a statement that says: "Sites **MUST** have a retention policy that establishes a destruction time table....The retention policy **MUST** be included in or linked from the site's human-readable privacy policy." This could give rise to both security risks and also litigation risks and goes significantly above laws or regulations for many site operators. Therefore, this should be changed to **SHOULD** or **MAY**

In 3.3.7, the text under **optional** appears to be overkill for the initial implementation. This is likely to lead to more errors and end-user confusion than it would be to help. This now reads:

Note that User Agents should be cautious about using the optional attribute in automated decision-making. If the optional attribute is associated with a data element directly controlled by the User Agent (such as the HTTP Referer header or cookies), the User Agent should make sure that this data is not transmitted to Web sites at which a data element is optional if the site's policy would not match a user's

preferences if the data element was required. Likewise, for data elements that users typically type into forms, user agents should alert users when a site's practices about optional data do not match their preferences.

Section 4. on Compact Policies appears to be the most incomplete, with many ideas raised and then not discussed. For example, Section 4.0 says:

In P3Pv1, compact policies contain policy information related to cookies only. Is this true? The web server is responsible for building a P3P compact policy to represent the cookies referenced in a full policy. The policy specified in a P3P compact policy applies to data stored within all cookies set in the same HTTP response as the compact policy, all cookies set by scripts associated with that HTTP response, and also to data linked to the cookies.

However there is no explanation of how a web server should accomplish this, how the web server should build a P3P compact policy to represent the cookies referenced, and also how it should deliver this if it were not to do so in a P3P header

Section 4.0 also raises ambiguity by saying what a User Agent SHOULD do, but offering no certainty that it will do this, or what the defaults should be if the User Agent cannot or chooses not to do this. Current language says:

Compact policies are summarized P3P policies that provide hints to user agents to enable the user agent to make quick, synchronous decisions about applying policy. Compact policies are a performance optimization that is **OPTIONAL** for either user agents or servers. User agents that are unable to obtain enough information from a compact policy to make a decision according to a user's preferences SHOULD fetch the full policy.

Section 4.2.1 on use of Access in Compact Policies illustrates one of the fundamental problems with the document. This would apply to both the cookie information in the full policies as well as the tokens in the compact policies.

Section 4.0 says that: "In P3Pv1, compact policies contain policy information related to cookies only." However, the options do not appear to relate to how cookies work. For example, many cookies can be accessed on the user machine. Other "cookie like objects" may simply capture NOI information for counts or for session performance. If this is a session cookie that disappears, what should the setting be, since there would be no access after the session is over.

This is why the document should go through each item from both a cookie and a Compact Policy perspective. The language and tokens available should also consider how cookies typically work.

It is hard to image Disputes or Remedies having use in many cookies. There should be an easy way to bypass these, for example, for Session Cookies.

The items in 4.2.7 on **RETENTION** are not very relevant to most cookies. These may be set to session, persistent, etc., especially if the user can remove these at any time.

Again 4.5 and 4.6 should make it very clear that the developer is only translating the "cookie policy" in to a Compact Policy. While a very seasoned programmer may pick this up, most non-technical users who may be questioning the accuracy of a Compact Policy would not.

The items in 5.3.1 talking to possibilities for defining different data structures and elements are meant to be helpful. However, the current explanations are likely to be beyond the reach of all but a few. Our recommendation is to simplify, and take away many of the risks for sites that are attempting to comply—at least for the first round.

It appears that very simple solutions are possible for many sites, even those with a very large number of data elements.

It also appears that there are some very punitive risks for some who may use these solutions.

Section 5.7.2 on Variable Category Data Elements/Structures, gets very complex. Perhaps the penalties from making minor mistakes could be reduced for the initial implementation. This is potentially a good tool, however, there needs to be some flexibility for making minor mistakes the first time.

Additional Suggestions

In 3.3.7, The DATA-GROUP and DATA elements, the text under optional should be rephrased so that the answers are intuitive. Should read:

"indicates whether or not the "session?" treats this data element as an "optional" field; "no" indicates that the data element is required, while "yes" indicates that the data element is not required. *The default is "no"*. The optional attribute is used only in policies (not in data schema definitions).

It may be helpful to review the standard structures against other database management and Customer Relationship Management (CRM) tools to ensure that these are consistent in terms of groupings and descriptions. Otherwise companies are likely to have separate descriptors that are inconsistent.

For example, 5.5.5. Telephones is likely to need a designator for Home or Work. Information in the "telecom" structure. This may be more likely to be compatible with the structure in other standard implementations.

Closing Comments

We appreciate the opportunity to submit these comments. Should you have questions, please contact me directly.

Sincerely,

Catherine A. Allen

CEO, BITS

The Financial Services Roundtable

805 15th Street NW, Suite 600

Washington DC 20005

(202) 289-4322

cathy@fsround.org

c: BITS Executive Committee and P3P Working Group