

# Settling: A Simplified Web Privacy Negotiation Scheme

Aaron Rankin

Carnegie Mellon University

<arankin@cmu.edu>

## Abstract

The Platform for Privacy Preferences (P3P) has emerged as a standard way to encode online privacy policies into a machine-readable format. P3P's use is currently limited to informing web users of website privacy policies, but there exists the potential for P3P to enable negotiation between web users and websites. Negotiation could yield more privacy for web users as sites compete in the tradeoff of value and quality of service versus user privacy. In defining P3P, negotiation was abandoned as it was assumed too complicated for web users. *Settling* offers a simpler approach to privacy negotiation, while potentially achieving the original goal of enhanced privacy.

## 1 Introduction

Research has shown the growing concern of users about how their personal information is used online. Interestingly this research indicates that users have less confidence in how online service providers handle their information than they have in traditional brick-and-mortar service providers and merchants [6]. Online providers commonly provide textual privacy policies, which are not effective for several reasons, such as a lack of standardization and being too verbose.

Many consumers say they would prefer if privacy policies were presented in a standard, easy-to read format [26]. The Platform for Privacy Preferences (P3P) has become the standard way of encoding privacy policies into a machine-readable format [1]. With P3P, privacy policies can be automatically retrieved and presented to users appropriately.

P3P is presently used in this limited fashion – presenting privacy policies to users in a standardized way. Other uses of P3P have been considered and discarded over time.

Privacy preference negotiation is among this discarded set due to complexity of implementation and use process [4].

The first P3P drafts in August 1999 included a negotiation component. Outlined in [7], this protocol would allow for a user or a user-agent to accept or reject certain site policy statements. If any are rejected, the interaction with the website is halted – a denial of service (DoS). Not only is this a demanding task for users, but it is obviously flawed. Web users wish to access services and site owners wish to offer them. Neither will happen if a DoS occurs.

Alternative strategies to the W3C's P3P negotiation protocol exist [7]. A common problem in all strategies is usability. Assuming that users do not want to negotiate manually with websites, a natural direction to take is for sites to simply accept and abide by users' preferences. *Settling* is just this, a protocol in which websites may offer the option of accepting users' preferences without any negotiation.

*Paper overview* The remainder of this paper is organized as follows: Section 2 provides non-technical overview of Settling. Section 3 details the technical issues of implementation and a prototype of Settling. Section 4 contains concluding remarks, unresolved issues and areas of future work. Appendix 1 presents a flowchart of the Settling protocol. Appendix 2 contains the P3P 1.0 XSD (XML schema definition) schema with Settling, and Appendix 3 has an example P3P policy file with Settling. Appendix 4 contains the Settling prototype preference XML file and Appendix 5 contains the XSD schema for this file.

## 2 Overview of Settling

Settling is a process whereby a user or an organization settles for the privacy preferences of the other. One property of Settling is called the *focus*. Focus levels dictate how compatible a service is with user privacy preferences. Settling has two focus levels:

**Organization-focused:** the organization will provide the service in question under the agreement that any data collected will be handled according to the organization's privacy policy.

**User-focused:** the organization will provide the service in question under the agreement that any data collected will be handled according to the user's privacy preferences.

The focus must be encoded into a P3P policy, which will require changes to the 1.0 specification [2].

### 2.1 The Protocol

Designed in response to the complex negotiation schemes proposed, Settling is a very simple interaction. Depending on user preferences, the process can be completely silent, being carried out automatically by the user-agent and the web server. Appendix 1 presents a flowchart of the protocol.

The basic use-case flow of Settling is as follows. A user visits a P3P-enabled website with a Settling-enabled P3P user-agent. The user-agent retrieves the website's P3P policy file and examines it to determine if user-focused Settling is supported. If the site does not and instead supports organization-focused Settling, the user/website interaction continues in the traditional manner, with the user implicitly accepting the website's policy. If the site does support user-focused Settling, the user-agent will check its application

preferences, which are set by the user, to determine which of two actions to take. The first action is simply to send the user's privacy preferences, which are encoded in the A P3P Preference Exchange Language 1.0 (APPEL1.0) [5] format, to the web server. If this action is the user's preference, the website will receive the user's preferences and tailor their service to abide by the user's preferences. The second possible action is to prompt the user, asking if they wish for their APPEL-encoded preferences to be sent to this website. Likewise, if the user chooses to send their preferences, the website will receive the user's preferences and tailor their service to abide by the user's preferences. Otherwise, the user/website interaction continues in the traditional manner, with the user implicitly accepting the website's policy. As the user browses this website and others, the Settling protocol is continually executed for each page that presents a new P3P policy.

Unless the user has chosen to be prompted at each Settling-enabled site, the process outlined above will be completely silent. In fact, the user need not be notified about any step, aside from the result, of the Settling protocol. They may remain focused on using the website, while remaining updated on whether or not their privacy preferences are being respected.

How a website upholds a user's preferences is up to its implementation. One strategy is to adjust the website's services to require less data collection, based on what information the user wishes to provide. Another strategy is simply to associate any collected data with the user's APPEL preferences. Upon performing some operation on that information, such as collecting email addresses to provide to a third party, each user's preferences are first consulted before any information is used. The second strategy presents a potentially difficult problem, computationally. Such a strategy could be an area of research for the database community. That is how to link information to privacy preferences such that queries uphold the

preferences and are efficient. One can envision this working similarly to access control in current databases.

### 3 Implementation Issues of Settling

#### 3.1 Design Considerations

Being a client/server interaction, a Settling implementation obviously requires design choices on both sides. In evaluating options, there are two very important factors to consider – standardization and the ease of implementation. Standardization is necessary to guarantee that users’ experiences are consistent across user-agents and websites. Ease of implementation is necessary to encourage user-agent developers and website owners to implement Settling.

Few design options exist for the client side. Assuming that Settling is a component of the P3P schema the most natural choice is to integrate Settling functionality into the P3P user-agent. Upon retrieving the P3P file, the user-agent can also execute its side of the protocol. This option was chosen for the Settling prototype outlined in section 3.3.

More options exist on the server side, each of which has different implementation implications. Because some server process must receive and store the APPEL file, the Settling component on the server must be an active entity. This is a major change to P3P, as it currently is implemented as XML (text) files.

One server-side option is to integrate Settling directly into the web server. Given a standardized API, Settling could be implemented as a service available on a standardized port. This service could be accessible via any remote invocation scheme, such as Java Remote Method Invocation [8]. Client user-agents could communicate with this service by conforming to the same standard.

This approach is not perfect. On the positive side, Settling will be implemented fewer times, as it is supported at the server

layer versus the application layer. On the negative side, web server vendors may not be interested in providing applications with support for privacy at their lower layer – it seems to be slightly out of their jurisdiction. However, other application mechanisms such as the encryption offered by the secure Hyper Text Transfer Protocol (HTTPS) via Secure Socket Layer (SSL) and others are implemented at the web server level. Therefore, implementing Settling at this level is a possibility.

A second server-side option is to implement Settling at the web application layer. Websites would have server-side scripts that the user-agent would communicate with via standard HTTP. An example of this would be to implement Settling within a Java Servlet [9].

This approach has one major implication: the client must know the location of the Settling application. Like P3P policies, this could be achieved with a well-known location [2]. This choice may be burdensome for web server administrators, however, as organizations follow proprietary conventions for file locations. Files such as server-side scripts, especially, require that they be executed from specific locations on the server. Requiring a specific directory to possess execute privileges may be unacceptable in some situations. A second approach is to allow the placement of server-side Settling code to be up to the discretion of the organization. By doing so, however, there must be a mechanism for informing the client of what that location is. This could be done by including such information with the Settling information within the P3P policy. Flexibility is the major selling point of this choice. This option was chosen for the Settling prototype outlined in section 3.3.

#### 3.2 Settling In the P3P Framework

Based on the client and server design decisions chosen above for the prototype, direct changes to both the P3P specification and to the

preference formats of user-agents will be required. In particular, it is necessary for web sites to express whether they support user-focused or organization-focused Settling. If they do support user-focused Settling, it is also necessary for them to express the URL of their server-side Settling application. On the client side, user-agents must support the APPEL preference standard.

Necessary changes to P3P include schematic changes, which will yield slightly different policy files. In particular, the P3P XML schema must now include an element for Settling – `SETTLING-NEGOTIATION`. This element will contain attributes – `focus` and `userFocusURL` – that will structure the data on what focus level the site supports (user or organization) as well as the URL of the Settling application if the site supports user-focused Settling.

```
...
<!-- Settling: Compatibility Data Type -->
<xsd:simpleType name='compatibilityType'>
  <xsd:restriction base='xsd:string'>
    <xsd:enumeration value='user' />
    <xsd:enumeration value='org' />
  </xsd:restriction>
</xsd:simpleType>
...
<element name='SETTLING-NEGOTIATION'>
  <complexType>
    <attribute name='focus'
              type='p3p:compatibilityType'
              use='required' />
    <attribute name='userFocusURL'
              type='xsd:string'
              use='optional' />
  </complexType>
</element>
...
```

**Figure 3.2-1**

Figure 3.2-1 illustrates an addition to the P3P schema for the `SETTLING-COMPATIBILITY` element as well as the `compatibilityType` datatype. These changes alone integrate Settling into the P3P standard. The full P3P 1.0 schema with Settling is presented in Appendix 2.

Implementing Settling within a P3P Policy is equally straightforward. As is evident from the schematic change, all Settling-specific information is encoded within one element, `SETTLING-COMPATIBILITY`, using two attributes, `focus` and `userFocusURL`.

```
...
<SETTLING-NEGOTIATION
focus="user"
userFocusURL="http://localhost:8080/P3PSettle
r/P3PSettlingServlet"/>
...
```

**Figure 3.2-2**

Figure 3.2-2 presents an example addition to a P3P policy. This example shows the website supporting user-focused Settling, with their server application for Settling at the URL `http://localhost:8080/P3PSettler/P3PSettlingServlet`. An example P3P policy from the W3C with Settling inserted is presented in Appendix 3.

Moving on to user-agents, APPEL or some other standard will have to be adopted as the privacy preference formats will have to be standardized in order to enable user-focused Settling. Many user-agents currently use proprietary rule-based languages. User-agents will also need to support several Settling preferences, which the user should be able to set. Currently, two simple options exist – `isSettlingEnabled` and `defaultAction`. `isSettlingEnabled` simply enables or disables Settling. `defaultAction` is whether the user wishes to be prompted for confirmation before their preferences are sent. Thus the two values for this option are “send” or “prompt”. For example, a user-agent could simply present users with a option pane, where users may configure the available preferences, by clicking a button. These interfaces must convey the implications of each choice to the user in an easy-to-understand and concise way. Moreover, user-agents will be responsible for presenting users with a confirmation mechanism (e.g., in a GUI environment, a

pop-up window) if the user wishes to be prompted at user-focused Settling sites.

### 3.3 A Java Prototype

As a proof-of-concept, a Settling prototype was developed and tested. Building the prototype allowed us to enumerate the various decision decisions as well as to refine the original Settling concept [10]. This implementation was not intended to reflect an exact production release of Settling functionality, but rather to demonstrate the concept during actual web browsing. Java was chosen as the implementation language simply due to the author's familiarity.

#### 3.3.1 The Client Module

A production implementation of Settling would integrate client-side functionality within the P3P user-agent. Several user-agents were considered for integration with this prototype – Microsoft Internet Explorer, AT&T Privacy Bird [3] – however, it was decided that due to unfamiliarity with their APIs, integration at that level was out of the scope of this prototype. Instead, a proxy model was chosen for the client module.

The module operates on a client port, and the client's web browser must be configured to use localhost:settlingport as its outgoing proxy. For example, if the client module operates on port 6503, the user's web browser must be configured to use localhost:6503 as its outgoing proxy. All outgoing web traffic from the web browser is then funneled through the Settling client module, where it takes two actions. The first action is to execute the Settling protocol with the web host that the user requested. The second action is to complete the original web request, whereby it presents the user with the content they requested.

The client is responsible for all of the active work within the Settling protocol. That is, it retrieves the P3P policy, determines if user-focused Settling is supported, then prompts the user or sends their APPEL

preferences to the server Settling application URL. These actions were all generally implemented as they were outlined in Section 3.2. The prototype does not provide functionality to manage either APPEL preferences or Settling preferences from within the application. Both preference files are XML, and it is expected that the user manually set their preferences by editing these files. The Settling preference file for this prototype is presented in Appendix 4, with its XSD schema in Appendix 5. Note that the proxy nature of this implementation required additional preferences, such as the port on which it will run. In the case of the user prompt, a Java Swing confirmation window is used, as is presented in Figure 3.3.1-1. As the prototype does not integrate with the user's software in any way, it does not provide any notification of user-focused Settling being supported or unsupported within the user-agent or the browser. Instead, the prototype has the server-module inform the user of this state and displays status updates to the Java console.



Figure 3.3.1-1

#### 3.3.2 The Server Module

Based the design choices from Section 3.1, the prototype's server module is much like a production implementation. To demonstrate server-side Settling functionality, only two new components, in addition to the Settling-enabled P3P policy, are needed – a page that the user wishes to visit and the Settling application.

The page that the user wishes to visit should simply check to see if the server has enabled a Settling-specific experience for the user. In the case of the prototype, this is simply a session state Boolean variable, which

is true when APPEL preferences have been received and false otherwise. A production system would presumably handle this in a more complex fashion, as user preferences would be linked to their data in some fashion.

The prototype's server-side Settling application is a Java Servlet, which receives APPEL preferences via HTTP from the client, at which point it sets the server-side state variable indicating that Settling is enabled for that user session. Again, a production implementation would differ from this in that the application would be responsible for linking the APPEL preferences to any data entered in that user session, or even future sessions from that same user.

### 3.4 Unresolved Issues

Several issues remain unresolved in the Settling framework. Two of the issues are user-related became apparent through minimal user testing, which was carried out in an unofficial cognitive walkthrough [11]. The final issue is a flaw in the protocol.

The first issue is cognitive on the part of the user and occurs when the prompt window appears (see Figure 3.3.1-1). Though the window states, "Do you wish to send your privacy preferences to this site," a user felt that this meant, "Do you wish to agree with this site's privacy policy." A solution to this issue could be simply to limit the number of prompts that a user will see, assuming that they have set the preference to receive prompts. In the case where the site has received the user's preferences in the past, they could be automatically sent. This behavior could be controlled by a user preference.

The second issue is one where the user is somewhat deceived by the Settling system. Psychologically, one feels that their privacy is being protected by such a system. However, giving the user the option of not sending their privacy preferences creates the possibility of less privacy. Obviously, a site, which does not have a user's preferences, has no way of abiding by their wishes. The prompt option is

intended to be an extra layer of privacy, assuming that some personal information exists within a set of privacy preferences. However, a user may lose more privacy than they would by revealing their preferences, by not revealing them. Consider even the example of a user that is very cautious when giving personal information to the site. Their browsing path may still be tracked, as in where they clicked, where this brought them and when, simply via cookies.

The third issue again is a major flaw in the Settling protocol – a lack of enforceability. P3P is legally binding as it represents a privacy policy. Moreover, it is static and lacks ambiguity. The Settling component in P3P needs to be dynamic for each user, as it must reflect the decision of the Settling protocol (whether to abide by the site's policy or the user's preferences). A crude solution to this is to store a P3P policy with the Settling decision and possibly the user's preferences somehow. These policies must then be associated with any data collected from that user, by some means (e.g., relational databases).

## 4 Conclusions and Future Work

This paper has considered P3P negotiation with regard to the flaws present in strategies proposed thus far. In response, we propose *Settling*, a reduced negotiation scheme. Settling provides the option for websites to uphold user privacy policies, thereby offering greater privacy. The formal economic rationale for websites to offer this option was not presented, however it was assumed that given users' concerns about personal privacy, websites would benefit from a competition of service value versus personal privacy.

To examine the Settling concept better, a Java prototype was developed. This allowed us to enumerate design considerations and then choose the most appropriate options. In using the prototype, we found the Settling experience to be non-intrusive, only prompting the user once per webpage, if they wished to

be prompted. This greatly differentiates Settling from other proposed schemes, which have a very demanding user interaction requirement.

Several issues did arise from working with the prototype, as well as from rethinking the protocol in general. These were: 1) a lack of user awareness as to what was actually taking place; 2) unintentionally deceiving the user into thinking they were achieving more privacy by not revealing their preferences, when in fact they may be losing more privacy than was gained by hiding their preferences; 3) Settling not being legally binding in its current state. No elegant solutions to these issues exist as of yet, and are areas for future work.

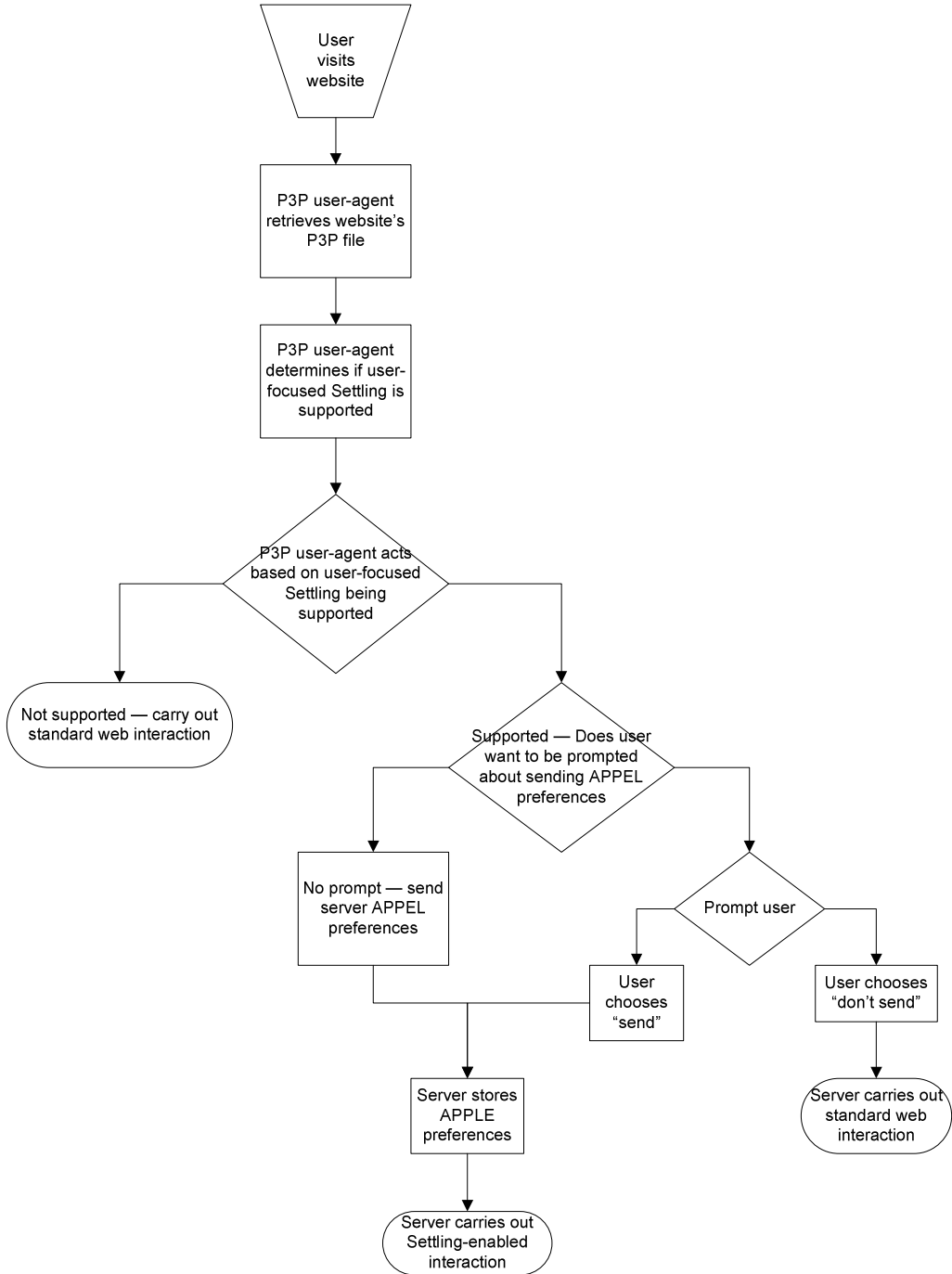
Other future work was also identified along the way. The first major challenge is a standardization of Settling. Our prototype suggested certain design choices for the client and server, as well as integration with P3P. There exists the potential for cleaner designs, however. A second issue is the action a website will take upon Settling with a client. We proposed two strategies, but others may too be plausible. A third area left to further research is the economic rationale for a website to adopt Settling. We assume that a formal reason exists, but do not pursue it.

Finally, previously unmentioned is a possible enhancement to Settling that is quite significant. Settling presently occurs at the privacy policy level. There exists the possibility to settle also at the policy line (or “field”) level. Organizations would choose which aspects of their P3P policies they wish to be user-focused and which others are to be organization-focused. This would provide organizations with more flexibility, potentially making the concept more easily adopted. How this would be implemented, in terms of client modules, server modules and P3P changes, is undetermined. In addition, how these changes will affect how users must interface with the Settling system is also a question.

## References

- [1] *Platform for Privacy Preferences (P3P) Project: P3P Public Overview*. W3C. <http://www.w3.org/P3P/>.
- [2] The Platform for Privacy Preferences 1.0 (P3P1.0) Specification. Cranor, L., Langheinrich, M., Marchiori, M., Presler-Marshall, M., and Reagle, J. World Wide Web Consortium Recommendation, April 2002. <http://www.w3.org/TR/P3P/>.
- [3] AT&T Privacy Bird. AT&T Research. <http://www.privacybird.com/>.
- [4] Removing Data Transfer from P3P. W3C. <http://www.w3.org/P3P/data-transfer.html>.
- [5] A P3P Preference Exchange Language 1.0 (APPEL1.0). Lorrie Cranor, Marc Langheinrich, Massimo Marchiori. <http://www.w3.org/TR/P3P-preferences/>.
- [6] *Commerce, Communication, and Privacy Online, A National Survey of Computer Users* (1997) (hereinafter referred to as "*Westin Survey*") at ix. Louis Harris & Associates and Dr. Alan F. Westin,
- [7] Privacy Server Protocol: A Short Summary. Robert Thibadeau. <<http://yuan.ecom.cmu.edu/psp/SummaryInterop.PDF>>.
- [8] Java Remote Method Invocation (Java RMI). Sun Microsystems. <<http://java.sun.com/products/jdk/rmi/>>.
- [9] Java Servlet Technology. Sun Microsystems. <<http://java.sun.com/products/servlet/>>.
- [10] P3P Enforcement and Usability: The Present State and Recommendations for Improvement. Aaron Rankin. <http://www.obermayer.org/~aaron/papers/Aaron%20Rankin%20-%20P3P%20Enforcement%20and%20Usability%20-%20The%20Present%20State%20and%20Recommendations%20for%20Improvement.pdf>
- [11] Performing a Cognitive Walkthrough. <<http://www.cc.gatech.edu/computing/classes/cs3302/documents/cog.walk.html>>.

## Appendix 1: Flowchart of the Settling Protocol



## Appendix 2: P3P 1.0 XML Schema (XSD) with Settling

```

<?xml version='1.0' encoding='UTF-8'?>
<schema
  xmlns='http://www.w3.org/2001/XMLSchema'
  xmlns:p3p='http://www.w3.org/2002/01/P3Pv1'
  targetNamespace='http://www.w3.org/2002/01/P3Pv1'
  elementFormDefault='qualified'>

  <!-- enabling xml:lang attribute -->
  <import
    namespace='http://www.w3.org/XML/1998/namespace'
  />

  schemaLocation='http://www.w3.org/2001/xml.xsd'
  />

  <!-- Basic P3P Data Type -->
  <simpleType name='yes_no'>
    <restriction base='string'>
      <enumeration value='yes' />
      <enumeration value='no' />
    </restriction>
  </simpleType>

  <!-- Settling: Compatibility Data Type -->
  <xsd:simpleType name='compatibilityType'>
    <xsd:restriction base='xsd:string'>
      <xsd:enumeration value='user' />
      <xsd:enumeration value='org' />
    </xsd:restriction>
  </xsd:simpleType>

  <!-- ***** Policy Reference ***** -->
  <!-- ***** META ***** -->
  <element name='META'>
    <complexType>
      <sequence>
        <element ref='p3p:EXTENSION' minOccurs='0'
          maxOccurs='unbounded' />
        <element ref='p3p:POLICY-REFERENCES' />
        <element ref='p3p:POLICIES'
          minOccurs='0' />
        <element ref='p3p:EXTENSION' minOccurs='0'
          maxOccurs='unbounded' />
      </sequence>
      <attribute ref='xml:lang' use='optional' />
    </complexType>
  </element>

  <!-- ***** POLICY-REFERENCES ***** -->
  <element name='POLICY-REFERENCES'>
    <complexType>
      <sequence>
        <element ref='p3p:EXPIRY' minOccurs='0' />
        <element ref='p3p:POLICY-REF'
          minOccurs='0' maxOccurs='unbounded' />
        <element ref='p3p:HINT' minOccurs='0'
          maxOccurs='unbounded' />
        <element ref='p3p:EXTENSION' minOccurs='0'
          maxOccurs='unbounded' />
      </sequence>
    </complexType>
  </element>

  <element name='POLICY-REF'>
    <complexType>
      <sequence>
        <element name='INCLUDE'
          minOccurs='0'
          maxOccurs='unbounded'
          type='anyURI' />
        <element name='EXCLUDE'
          minOccurs='0'
          maxOccurs='unbounded'
          type='anyURI' />
        <element name='COOKIE-INCLUDE'
          minOccurs='0'
          maxOccurs='unbounded'
          type='p3p:cookie-element' />
        <element name='COOKIE-EXCLUDE'
          minOccurs='0'
          maxOccurs='unbounded'
          type='p3p:cookie-element' />
        <element name='METHOD'
          minOccurs='0'
          maxOccurs='unbounded'
          type='anyURI' />
        <element ref='p3p:EXTENSION'
          minOccurs='0'
          maxOccurs='unbounded' />
      </sequence>
      <attribute name='about' type='anyURI'
        use='required' />
    </complexType>
  </element>

  <complexType name='cookie-element'>
    <attribute name='name' type='string'
      use='optional' />
    <attribute name='value' type='string'
      use='optional' />
    <attribute name='domain' type='string'
      use='optional' />
    <attribute name='path' type='string'
      use='optional' />
  </complexType>

  <!-- ***** HINT ***** -->
  <element name='HINT'>
    <complexType>
      <attribute name='scope' type='string'
        use='required' />
      <attribute name='path' type='string'
        use='required' />
    </complexType>
  </element>

  <!-- ***** POLICIES ***** -->
  <element name='POLICIES'>
    <complexType>
      <sequence>
        <element ref='p3p:EXPIRY' minOccurs='0' />
        <element ref='p3p:DATASchema'
          minOccurs='0' />
        <element ref='p3p:POLICY' minOccurs='0'
          maxOccurs='unbounded' />
      </sequence>
      <attribute ref='xml:lang' use='optional' />
    </complexType>
  </element>

```

```

</element>
<!-- ***** EXPIRY ***** -->
<element name='EXPIRY'>
  <complexType>
    <attribute name='max-age'
type='nonNegativeInteger' use='optional' />
    <attribute name='date' type='string'
use='optional' />
  </complexType>
</element>

<!-- ***** Policy ***** -->
<!-- ***** POLICY ***** -->
<element name='POLICY'>
  <complexType>
    <sequence>
      <element ref='p3p:EXTENSION' minOccurs='0'
maxOccurs='unbounded' />
      <element ref='p3p:TEST' minOccurs='0' />
      <element ref='p3p:ENTITY' />
      <element ref='p3p:ACCESS' />
      <element ref='p3p:DISPUTES-GROUP'
minOccurs='0' />
      <element ref='p3p:STATEMENT'
maxOccurs='unbounded' />
      <element ref='p3p:EXTENSION' minOccurs='0'
maxOccurs='unbounded' />
      <element ref='p3p:COMPATIBILITY'
minOccurs='0' maxOccurs='1' />
    </sequence>
    <attribute name='discuri' type='anyURI'
use='required' />
    <attribute name='opturi' type='anyURI'
use='optional' />
    <attribute name='name' type='ID'
use='required' />
    <attribute ref='xml:lang' use='optional' />
  </complexType>
</element>

<!-- ***** TEST ***** -->
<element name='TEST'>
  <complexType />
</element>

<!-- ***** ENTITY ***** -->
<element name='ENTITY'>
  <complexType>
    <sequence>
      <element ref='p3p:EXTENSION' minOccurs='0'
maxOccurs='unbounded' />
      <element name='DATA-GROUP'>
        <complexType>
          <sequence>
            <element name='DATA' type='p3p:data-in-
entity' maxOccurs='unbounded' />
          </sequence>
        </complexType>
      </element>
      <element ref='p3p:EXTENSION' minOccurs='0'
maxOccurs='unbounded' />
    </sequence>
  </complexType>
</element>

  <complexType name='data-in-entity'
mixed='true'>
    <attribute name='ref' type='anyURI'
use='required' />
  </complexType>
</complexType>

<!-- ***** ACCESS ***** -->
<element name='ACCESS'>
  <complexType>
    <sequence>
      <element ref='p3p:EXTENSION' minOccurs='0'
maxOccurs='unbounded' />
      <choice>
        <element name='nonident'
type='p3p:access-value' />
        <element name='ident-contact'
type='p3p:access-value' />
        <element name='other-ident'
type='p3p:access-value' />
        <element name='contact-and-other'
type='p3p:access-value' />
        <element name='all' type='p3p:access-
value' />
        <element name='none' type='p3p:access-
value' />
      </choice>
      <element ref='p3p:EXTENSION' minOccurs='0'
maxOccurs='unbounded' />
    </sequence>
  </complexType>
</element>

  <complexType name='access-value' />

<!-- ***** DISPUTES ***** -->
<element name='DISPUTES-GROUP'>
  <complexType>
    <sequence>
      <element ref='p3p:EXTENSION' minOccurs='0'
maxOccurs='unbounded' />
      <element ref='p3p:DISPUTES'
maxOccurs='unbounded' />
      <element ref='p3p:EXTENSION' minOccurs='0'
maxOccurs='unbounded' />
    </sequence>
  </complexType>
</element>

  <element name='DISPUTES'>
    <complexType>
      <sequence>
        <element ref='p3p:EXTENSION' minOccurs='0'
maxOccurs='unbounded' />
        <choice minOccurs='0'>
          <sequence>
            <element ref='p3p:LONG-DESCRIPTION' />
            <element ref='p3p:IMG' minOccurs='0' />
            <element ref='p3p:REMEDIES'
minOccurs='0' />
            <element ref='p3p:EXTENSION'
minOccurs='0' maxOccurs='unbounded' />
          </sequence>
          <sequence>
            <element ref='p3p:IMG' />
            <element ref='p3p:REMEDIES'
minOccurs='0' />
            <element ref='p3p:EXTENSION'
minOccurs='0' maxOccurs='unbounded' />
          </sequence>
          <sequence>
            <element ref='p3p:REMEDIES' />
            <element ref='p3p:EXTENSION'
minOccurs='0' maxOccurs='unbounded' />
          </sequence>
        </choice>
      </sequence>
    </complexType>
  </element>

```

```

    </sequence>
    <attribute name='resolution-type'
use='required'>
    <simpleType>
    <restriction base='string'>
    <enumeration value='service'>/>
    <enumeration value='independent'>/>
    <enumeration value='court'>/>
    <enumeration value='law'>/>
    </restriction>
    </simpleType>
    </attribute>
    <attribute name='service' type='anyURI'
use='required'>
    <attribute name='verification'
type='string' use='optional'>/>
    <attribute name='short-description'
type='string' use='optional'>/>
    </complexType>
  </element>

<!-- ***** LONG-DESCRIPTION ***** -->
  <element name='LONG-DESCRIPTION'>
  <simpleType>
  <restriction base='string'>/>
  </simpleType>
  </element>

<!-- ***** IMG ***** -->
  <element name='IMG'>
  <complexType>
  <attribute name='src' type='anyURI'
use='required'>/>
  <attribute name='width'
type='nonNegativeInteger' use='optional'>/>
  <attribute name='height'
type='nonNegativeInteger' use='optional'>/>
  <attribute name='alt' type='string'
use='required'>/>
  </complexType>
  </element>

<!-- ***** REMEDIES ***** -->
  <element name='REMEDIES'>
  <complexType>
  <sequence>
  <element ref='p3p:EXTENSION' minOccurs='0'
maxOccurs='unbounded'>/>
  <choice maxOccurs='unbounded'>
  <element name='correct'
type='p3p:remedies-value'>/>
  <element name='money' type='p3p:remedies-
value'>/>
  <element name='law' type='p3p:remedies-
value'>/>
  </choice>
  <element ref='p3p:EXTENSION' minOccurs='0'
maxOccurs='unbounded'>/>
  </sequence>
  </complexType>
  </element>

  <complexType name='remedies-value'>/>

<!-- ***** STATEMENT ***** -->
  <element name='STATEMENT'>
  <complexType>
  <sequence>
  <element ref='p3p:EXTENSION' minOccurs='0'
maxOccurs='unbounded'>/>
  </sequence>
  </complexType>
  </element>

  <element name='CONSEQUENCE' minOccurs='0'
type='string'>/>
  <choice>
  <sequence>
  <element ref='p3p:PURPOSE'>/>
  <element ref='p3p:RECIPIENT'>/>
  <element ref='p3p:RETENTION'>/>
  <element name='DATA-GROUP'
type='p3p:data-group-type'
maxOccurs='unbounded'>/>
  </sequence>
  <sequence>
  <element name='NON-IDENTIFIABLE'>/>
  <element ref='p3p:PURPOSE'
minOccurs='0'>/>
  <element ref='p3p:RECIPIENT'
minOccurs='0'>/>
  <element ref='p3p:RETENTION'
minOccurs='0'>/>
  <element name='DATA-GROUP'
type='p3p:data-group-type' minOccurs='0'
maxOccurs='unbounded'>/>
  </sequence>
  </choice>
  <element ref='p3p:EXTENSION' minOccurs='0'
maxOccurs='unbounded'>/>
  </sequence>
  </complexType>
  </element>

<!-- ***** PURPOSE ***** -->
  <element name='PURPOSE'>
  <complexType>
  <sequence>
  <element ref='p3p:EXTENSION' minOccurs='0'
maxOccurs='unbounded'>/>
  <choice maxOccurs='unbounded'>
  <element name='current'
type='p3p:purpose-value'>/>
  <element name='admin' type='p3p:purpose-
value'>/>
  <element name='develop'
type='p3p:purpose-value'>/>
  <element name='tailoring'
type='p3p:purpose-value'>/>
  <element name='pseudo-analysis'
type='p3p:purpose-value'>/>
  <element name='pseudo-decision'
type='p3p:purpose-value'>/>
  <element name='individual-analysis'
type='p3p:purpose-value'>/>
  <element name='individual-decision'
type='p3p:purpose-value'>/>
  <element name='contact'
type='p3p:purpose-value'>/>
  <element name='historical'
type='p3p:purpose-value'>/>
  <element name='telemarketing'
type='p3p:purpose-value'>/>
  <element name='other-purpose'>
  <complexType mixed='true'>
  <attribute name='required'
use='optional' type='p3p:required-value'>/>
  </complexType>
  </element>
  </choice>
  </sequence>
  </complexType>
  </element>
  </choice>
  </sequence>
  </complexType>
  </element>

```

```

<simpleType name='required-value'>
  <restriction base='string'>
    <enumeration value='always' />
    <enumeration value='opt-in' />
    <enumeration value='opt-out' />
  </restriction>
</simpleType>

<complexType name='purpose-value'>
  <attribute name='required' use='optional'
type='p3p:required-value' default='always' />
</complexType>

<!-- ***** RECIPIENT ***** -->
<element name='RECIPIENT'>
  <complexType>
    <sequence>
      <element ref='p3p:EXTENSION' minOccurs='0'
maxOccurs='unbounded' />
      <choice maxOccurs='unbounded'>
        <element name='ours'>
          <complexType>
            <sequence>
              <element ref='p3p:recipient-
description' minOccurs='0'
maxOccurs='unbounded' />
            </sequence>
          </complexType>
        </element>
        <element name='same' type='p3p:recipient-
value' />
        <element name='other-recipient'
type='p3p:recipient-value' />
        <element name='delivery'
type='p3p:recipient-value' />
        <element name='public'
type='p3p:recipient-value' />
        <element name='unrelated'
type='p3p:recipient-value' />
      </choice>
      <element ref='p3p:EXTENSION' minOccurs='0'
maxOccurs='unbounded' />
    </sequence>
  </complexType>
</element>

<complexType name='recipient-value'>
  <sequence>
    <element ref='p3p:recipient-description'
minOccurs='0' maxOccurs='unbounded' />
  </sequence>
  <attribute name='required' use='optional'
type='p3p:required-value' />
</complexType>

<element name='recipient-description'>
  <complexType mixed='true' />
</element>

<!-- ***** RETENTION ***** -->
<element name='RETENTION'>
  <complexType>
    <sequence>
      <element ref='p3p:EXTENSION' minOccurs='0'
maxOccurs='unbounded' />
      <choice>
        <element name='no-retention'
type='p3p:retention-value' />
        <element name='stated-purpose'
type='p3p:retention-value' />
        <element name='legal-requirement'
type='p3p:retention-value' />
        <element name='indefinitely'
type='p3p:retention-value' />
        <element name='business-practices'
type='p3p:retention-value' />
      </choice>
      <element ref='p3p:EXTENSION' minOccurs='0'
maxOccurs='unbounded' />
    </sequence>
  </complexType>
</element>

<complexType name='retention-value' />

<!-- ***** DATA ***** -->
<complexType name='data-group-type'>
  <sequence>
    <element ref='p3p:EXTENSION' minOccurs='0'
maxOccurs='unbounded' />
    <element name='DATA' type='p3p:data-in-
statement' maxOccurs='unbounded' />
    <element ref='p3p:EXTENSION' minOccurs='0'
maxOccurs='unbounded' />
  </sequence>
  <attribute name='base' type='anyURI'
use='optional'
default='http://www.w3.org/TR/P3P/base' />
</complexType>

<complexType name='data-in-statement'
mixed='true'>
  <sequence minOccurs='0'
maxOccurs='unbounded'>
    <element ref='p3p:CATEGORIES' />
  </sequence>
  <attribute name='ref' type='anyURI'
use='required' />
  <attribute name='optional' use='optional'
default='no' type='p3p:yes_no' />
</complexType>

<!-- ***** Data Schema ***** -->
<!-- ***** DATASHEMA ***** -->
<element name='DATASHEMA'>
  <complexType>
    <choice minOccurs='0'
maxOccurs='unbounded'>
      <element ref='p3p:DATA-DEF' />
      <element ref='p3p:DATA-STRUCT' />
      <element ref='p3p:EXTENSION' />
    </choice>
    <attribute ref='xml:lang' use='optional' />
  </complexType>
</element>

<element name='DATA-DEF' type='p3p:data-
def' />
<element name='DATA-STRUCT' type='p3p:data-
def' />

<complexType name='data-def'>
  <sequence>
    <element ref='p3p:CATEGORIES'
minOccurs='0' />
    <element ref='p3p:LONG-DESCRIPTION'
minOccurs='0' />
  </sequence>
  <attribute name='name' type='ID'
use='required' />

```

```

    <attribute name='structref' type='anyURI'
use='optional'/>
    <attribute name='short-description'
type='string' use='optional'/>
  </complexType>
</complexType>
</element>
</schema>

<!-- ***** CATEGORIES ***** -->
<element name='CATEGORIES'>
  <complexType>
    <choice maxOccurs='unbounded'>
      <element name='physical'
type='p3p:categories-value'/>
      <element name='online'
type='p3p:categories-value'/>
      <element name='uniqueid'
type='p3p:categories-value'/>
      <element name='purchase'
type='p3p:categories-value'/>
      <element name='financial'
type='p3p:categories-value'/>
      <element name='computer'
type='p3p:categories-value'/>
      <element name='navigation'
type='p3p:categories-value'/>
      <element name='interactive'
type='p3p:categories-value'/>
      <element name='demographic'
type='p3p:categories-value'/>
      <element name='content'
type='p3p:categories-value'/>
      <element name='state'
type='p3p:categories-value'/>
      <element name='political'
type='p3p:categories-value'/>
      <element name='health'
type='p3p:categories-value'/>
      <element name='preference'
type='p3p:categories-value'/>
      <element name='location'
type='p3p:categories-value'/>
      <element name='government'
type='p3p:categories-value'/>
      <element name='other-category'
type='string'/>
    </choice>
  </complexType>
</element>

<complexType name='categories-value'/>

<!-- ***** EXTENSION ***** -->
<element name='EXTENSION'>
  <complexType mixed='true'>
    <choice minOccurs='0'
maxOccurs='unbounded'>
      <any minOccurs='0' maxOccurs='unbounded'
processContents='skip'/>
    </choice>
    <attribute name='optional' use='optional'
default='yes' type='p3p:yes_no'/>
  </complexType>
</element>

<!-- ***** SETTling-NEGOTIATION (for
Settling) ***** -->
<element name='SETTLING-NEGOTIATION'>
  <complexType>
    <attribute name='focus'
type='p3p:compatibilityType' use='required'/>
    <attribute name='userFocusURL'
type='xsd:string' use='optional'/>

```

### Appendix 3: An Example P3P Policy with Settling, from W3C

```

<?xml version="1.0"?>
<POLICIES xmlns="P3Pv1.Settling.xsd">
  <EXPIRY max-age="604800"/>
  <POLICY name="public"
    discuri="http://www.w3.org/Consortium/Legal/privacy-statement#Public">
    <SETTLING-NEGOTIATION
      focus="user" userFocusURL="http://localhost:8080/P3PSettler/P3PSettlingServlet"/>
    <!-- Generated by GVIM and Rigo 1.0 -->
    <ENTITY>
      <DATA-GROUP>
        <DATA ref="#business.name">World Wide Web Consortium</DATA>
        <DATA ref="#business.contact-info.postal.name">MIT/LCS</DATA>
        <DATA ref="#business.contact-info.postal.street">545 Technology Square</DATA>
        <DATA ref="#business.contact-info.postal.postalcode">02143</DATA>
        <DATA ref="#business.contact-info.postal.city">Cambridge MA</DATA>
        <DATA ref="#business.contact-info.postal.country">USA</DATA>
        <DATA ref="#business.contact-info.postal.name">INRIA/Sophia Antipolis</DATA>
        <DATA ref="#business.contact-info.postal.street">2004 Routes des
Lucioles</DATA>
        <DATA ref="#business.contact-info.postal.postalcode">F-06902</DATA>
        <DATA ref="#business.contact-info.postal.city">Sophia Antipolis</DATA>
        <DATA ref="#business.contact-info.postal.country">FRANCE</DATA>
        <DATA ref="#business.contact-info.postal.name">Keio University</DATA>
        <DATA ref="#business.contact-info.postal.street">Shonan Fujisawa Campus</DATA>
        <DATA ref="#business.contact-info.postal.postalcode">252-8520</DATA>
        <DATA ref="#business.contact-info.postal.city">5322 Endo, Fujisawa-shi,
Kanagawa</DATA>
        <DATA ref="#business.contact-info.postal.country">JAPAN</DATA>
        <DATA ref="#business.contact-info.online.email">site-policy@w3.org</DATA>
        <DATA ref="#business.contact-info.telecom.telephone.intcode">1</DATA>
        <DATA ref="#business.contact-info.telecom.telephone.loccode">617</DATA>
        <DATA ref="#business.contact-info.telecom.telephone.number">2532613</DATA>
        <DATA ref="#business.contact-info.online.email">site-policy@w3.org</DATA>
        <DATA ref="#business.contact-info.online.uri">http://www.w3.org</DATA>
        <DATA ref="#business.contact-info.telecom.telephone.intcode">1</DATA>
        <DATA ref="#business.contact-info.telecom.telephone.loccode">617</DATA>
        <DATA ref="#business.contact-info.telecom.telephone.number">2532613</DATA>
      </DATA-GROUP>
    </ENTITY>

    <ACCESS>
      <nonident/>
    </ACCESS>

    <DISPUTES-GROUP>
      <DISPUTES resolution-type="service" service="http://www.w3.org/"
        short-description="site-policy@w3.org">
        <LONG-DESCRIPTION>The Webmaster and our Communications Team
will carefully consider the input and correct errors. If you
discover privacy invasive behavior, please don't hesitate to
contact us.
</LONG-DESCRIPTION>
        <IMG src="http://www.w3.org/Icons/WWW/w3c_home" width="72" height="48"
alt="Logo World Wide Web Consortium"/>
        <REMEDIES><correct/></REMEDIES>
      </DISPUTES>
    </DISPUTES-GROUP>

    <STATEMENT>

    <CONSEQUENCE>
      We collect normal Web-Logs. They are used for Server
administration, Web protocol research, Statistics of usage and
security. Those logs are anonymized after one month.
    </CONSEQUENCE>

```

```
<PURPOSE>
  <current/>
  <admin/>
  <develop/>
</PURPOSE>

<RECIPIENT>
  <ours>
    <recipient-description>
      The logs and other information go to our system-team. They keep logs
      confidential so they are not accessible for all W3C
    </recipient-description>
  </ours>
</RECIPIENT>

<RETENTION>
  <business-practices/>
</RETENTION>

<DATA-GROUP>
  <DATA ref="#dynamic.clickstream" />
  <DATA ref="#dynamic.http.useragent"/>
  <DATA ref="#dynamic.http.referer" />
</DATA-GROUP>
</STATEMENT>
</POLICY>
</POLICIES>
```

## Appendix 4: Settling Prototype Preference XML File

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<settlerClientPrefs
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="settler-client-prefs.xsd">
  <metaConfiguration
    port="6503"
    isSettlerEnabled="true"/>
  <userConfiguration
    defaultAction="prompt"/>
</settlerClientPrefs>
```

## Appendix 5: Settling Prototype Preference XML File XSD Schema

```

<?xml version="1.0" encoding="utf-16"?>
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="settlerClientPrefs">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="metaConfiguration">
          <xs:complexType>
            <xs:attribute name="port" type="xs:unsignedShort"
              use="required" />
            <xs:attribute name="isSetterEnabled" type="xs:boolean"
              use="required" />
          </xs:complexType>
        </xs:element>
        <xs:element name="userConfiguration">
          <xs:complexType>
            <xs:attribute name="defaultAction" use="required">
              <xs:simpleType>
                <xs:restriction base="xs:string">
                  <xs:enumeration value="send"/>
                  <xs:enumeration value="prompt"/>
                </xs:restriction>
              </xs:simpleType>
            </xs:attribute>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>

```