

Proposal: Agent-Of Domain Relationships

Prepared for W3C P3P 1.1 Working Group
Jack Humphrey (jhumphrey@coremetrics.com)
October 2003

Introduction

As part of the P3P 1.1 effort, this document describes modifications to the P3P specification that would allow user agents to recognize when hosts in different domains have an agent-client relationship in which data is collected by the agent solely on behalf of the client. They build on the modifications suggested in the “Same-Entity Domain Relationships” proposal, which covers multiple domains owned by the same entity.

This document contains an overview of the proposed modifications but not the specification-level details of the modifications, which will be provided in a subsequent document.

Proposed Additions to Policy Reference Files

Consider a site `example.com` that uses a data collection service provided by another company, whose site `sample.com` makes use of embedded image requests and cookies to collect data solely on behalf of its clients. `Sample.com` maintains no ownership of this data and has only administrative responsibilities for its use. We refer to this situation as an “agent of” relationship, as in “`sample.com` is an agent of `example.com`.”

The proposed mechanism allows the expression of the “agent of” relationship in much the same way as the “same entity” relationship, described in a separate proposal. For requests received on behalf of `example.com`, `sample.com` could return a P3P policyref header referring to `example.com`’s policy reference file, which would look something like this:

```
<META xmlns="http://www.w3.org/2002/01/P3Pv1">
  <POLICY-REFERENCES>
    <POLICY-REF about="/p3p/policy.xml#sample.com">
      <INCLUDE>*</INCLUDE>
    </POLICY-REF>
  </POLICY-REFERENCES>
  <KNOWN-HOSTS>
    <HOST name="*.sample.com" entity-type="AGENT"
  about="http://www.sample.com/p3p/policy.xml#default"/>
  </KNOWN-HOSTS>
</META>
```

This file refers to a P3P policy hosted by `example.com` that covers the data collected through the `sample.com` service. The `HOST` name attribute above indicates that `sample.com` is allowed to refer to this policy reference file, the `type` attribute indicates

that it is an agent acting on behalf of example.com, and the about attribute provides a URL for a default policy for the agent, which allows identification of the entity providing the agent service.

Proposed Additions to Support Compact Policies

Some user agents choose to only use compact policies to apply privacy preferences to cookies. Since compact policies do not allow the same level of expressiveness as policy reference files, they require a parallel mechanism to allow expression of “agent of” relationships. The proposed mechanism calls for the addition of two new HTTP P3P headers: agent-of and has-agent.

P3P agent-of Header

The P3P agent-of header allows a host to specify a list of space-delimited hostname qualifiers. This header denotes that the current host is providing a service that may involve collecting data solely on behalf of the listed hosts. This list has no direct mapping to the policy reference file but corresponds to the policy reference file(s) included in the P3P policyref header. In the “agent of” example, sample.com would return the header:

```
P3P: agent-of="*.example.com"
```

The P3P has-agent header allows a host to specify a list of space-delimited hostname qualifiers and URIs (separated by semicolons) that describe agent hosts that may collect data solely on behalf of the current host. This list must match the list of known hosts of type AGENT in the policy reference file. In the “agent of” example, example.com would return the header:

```
P3P: has-agent="*.sample.com;  
http://www.sample.com/p3p/policy.xml#default"
```

When evaluating compact policies, a user-agent should only consider one host to be an agent of another if the agent host has a matching agent-of hostname qualifier for the client host and the client host has a matching has-agent hostname qualifier.

Efficiency Concerns

For purposes of efficiency, hosts should not be required to return all hostname qualifiers for each of these new headers on every request. Instead they may tailor the header based on the request context, e.g. if sample.com acts as agent for 100 different hosts, it may return only “*.example.com” if it can glean that the request was referred from example.com.

Implications for User Agents

To take advantage of the new expressiveness provided by the proposed modifications, user agents should implement the following high-level rules:

1. Agent Of: Host B should be considered an agent collecting data solely on behalf of host A if:
 - a. Host A refers to a policy reference file on host B, and that policy reference file contains a KNOWN-HOSTS entry for host B with type AGENT, or
 - b. During compact policy evaluation, host B's P3P agent-of header contains a matching hostname qualifier for host A, and host A's P3P has-agent header contains a matching hostname qualifier for host B.
2. In the event of a verified "agent of" relationship, no extra privacy restrictions should be applied to either host.