Privacy Icons
The Platform for Privacy Preferences 1.1 (P3P1.1) Specification

W3C Working Group Note 13 November 2006

This Version:  
http://www.w3.org/TR/2006/NOTE-P3P11-20061113/

Latest Version:  
http://www.w3.org/TR/P3P11/

Previous Version:  
http://www.w3.org/TR/2006/WD-P3P11-20060210/

Editors:  
Rigo Wenning, W3C / ERCIM (rigo@w3.org)  
Matthias Schunter, IBM

Authors:  
Lorrie Cranor, CMU (P3P 1.0 & P3P 1.1)  
Brooks Dobbs, bdbobs at doubleclick.net, Doubleclick Inc. (P3P 1.1)  
Serge Egelman, CMU (P3P 1.1), serge at guanotronic.com  
Giles Hogben, Joint Research Center of the European Commission (P3P 1.1)  
Jack Humphrey, JHumphrey at coremetrics.com, Coremetrics  
Marc Langheinrich, ETH Zurich (P3P 1.0)  
Massimo Marchiori, W3C / MIT / University of Venice (P3P 1.0)  
Martin Presler-Marshall, IBM (P3P 1.0)  
Joseph Reagle, W3C/MIT (P3P 1.0)  
Matthias Schunter, IBM (P3P 1.1)  
David A. Stampley, David_Stampley at reyrey.com, Invited Expert  
Rigo Wenning, W3C
## The Acme Policy

<table>
<thead>
<tr>
<th>Types of Information</th>
<th>How We Use Your Information</th>
<th>Who We Share Your Information With</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>provide service &amp; maintain site</td>
<td>research &amp; development</td>
</tr>
<tr>
<td>contact information</td>
<td><img src="image" alt="" /></td>
<td><img src="image" alt="" /></td>
</tr>
<tr>
<td>cookies</td>
<td><img src="image" alt="" /></td>
<td><img src="image" alt="" /></td>
</tr>
<tr>
<td>demographic information</td>
<td><img src="image" alt="" /></td>
<td><img src="image" alt="" /></td>
</tr>
<tr>
<td>financial information</td>
<td><img src="image" alt="" /></td>
<td><img src="image" alt="" /></td>
</tr>
<tr>
<td>health information</td>
<td><img src="image" alt="" /></td>
<td><img src="image" alt="" /></td>
</tr>
<tr>
<td>preferences</td>
<td><img src="image" alt="" /></td>
<td><img src="image" alt="" /></td>
</tr>
<tr>
<td>purchasing information</td>
<td><img src="image" alt="" /></td>
<td><img src="image" alt="" /></td>
</tr>
<tr>
<td>social security number &amp; govt ID</td>
<td><img src="image" alt="" /></td>
<td><img src="image" alt="" /></td>
</tr>
<tr>
<td>your activity on this site</td>
<td><img src="image" alt="" /></td>
<td><img src="image" alt="" /></td>
</tr>
<tr>
<td>your location</td>
<td><img src="image" alt="" /></td>
<td><img src="image" alt="" /></td>
</tr>
</tbody>
</table>

**Understanding this privacy policy:**

- ![](image) we will use your information in this way
- ![](image) we will not use your information in this way unless you opt-out

**Contact us:**

- ![](image) call 1 888-888-8888
- ![](image) www.acme.com
Protection Against Suspected Forgery and Attack Sites Features. The Firefox forgery and attack protection feature displays a warning if the website you are visiting is suspected of impersonating a legitimate website (commonly referred to as a phishing or forgery website) or a site that infiltrates or damages a computer system without your informed consent, including, without limitation, any computer viruses, worms, trojan horses, spyware, computer contaminant and/or other malicious and unwanted software (commonly called an attack site or malware). By default, Firefox checks the web pages that you visit against a blacklist that is downloaded to your hard drive at regularly scheduled intervals (e.g., approximately twice per hour), the rate of frequency may change from time to time. The blacklist does not include the full URL of each suspicious site. Instead, each URL is hashed (obscured so it can’t be read) and then broken into portions. Only a portion of each hashed URL is included on the blacklist on your hard drive. If there is a match, Firefox will check with its third party provider to ensure that the website is still on the blacklist. The information sent between Firefox and its third party provider(s) are hashed URLs. In fact, multiple hashed URLs are sent with the real hash so that the third party provider(s) will not know what site you are visiting. If there is a match, Firefox displays either a “Reported Web Forgery” or “Reported Attack Site” alert, as applicable.

You may completely turn off the forgery and/or attack site protection features in Firefox’s preferences. If you do this, none of the information discussed here will be downloaded to your hard drive or sent to any third party service provider. An article in our Firefox Knowledge Base gives you information about changing your preferences.

Each time Firefox checks in with a third party provider to download a new blacklist, Non-Personal Information and Potentially Personal Information, such as the information that the browser sends every time you visit a website as well as the version number of the blacklist on your system, is sent to a third party provider. In order to safeguard your privacy, Firefox will not transmit the complete URL of web pages that you visit to anyone. While it is possible that a third party service provider may determine the actual URL from the hashed URL sent, Mozilla’s third party service providers have entered into a written agreement with Mozilla not to use any data or other information about or from users of Firefox for purposes other than to provide and maintain their service. In addition, in no event will these third party service providers correlate any Firefox user data with any other data collected through other products, services or web properties of that provider. These third party service providers may inform you about additional notices regarding their applicable privacy policies. (For example, see Google Safe Browsing Service in Mozilla Firefox Version 3.)
Product.
People do not know want they want.

We are the experts.
87%
Every time we ask the user a question they don’t understand or don’t care about, we have failed.
Respect the user?
With all of the work that’s been done before us, I wanted to touch on some of the way our thinking and position breaks from the mold.

**Bolt On Approach**

Privacy policies and Terms of Service are complex documents that encapsulate a lot of situation specific detail. The Creative Commons approach is to reduce the complexity of sharing to a small number of licenses from which you choose. That simply doesn’t work here. There are too many edge cases and specifics that each company has to put into their privacy policy. There can be no catch all better plans. We seem to have lost before we begun. There’s another approach.

Here’s where we stand. Companies need to write their own privacy policies/terms of service, replete with company specific detail. Why? Because a small number of licenses can’t capture the required complexity. The problem is that for everyday people, reading and understanding those necessarily complex privacy policies is time consuming and high impossible.

Here’s the solution: Create a set of easily understood Privacy icons that “bolt on to” a privacy policy.

When you add a Privacy icon to your privacy policy it says the equivalent of “No matter what the rest of this privacy policy says, the following is true and preempt anything else in this document.”. The Privacy icon makes an iron-clad guarantee about some portion of how a company treats your data.

For example, if a privacy policy includes the icon for “None of your data is sold or shared with 3rd parties”, then no matter what the privacy policy says in the small print, it gets preempted by the icon and the company is legally bound to never sharing or selling your data. Of course, the set of icons still needs to be decided (we’ll be having a workshop on the 27th of January to help figure it out).
With all of the work that's been done before us, I wanted to touch on some of the way our thinking and position breaks from the mold.

**Focus**

**Bolt On Approach**

Privacy policies and Terms of Service are complex documents that encapsulate a lot of situation-specific detail. The Creative Commons approach is to reduce the complexity of sharing to a small number of licenses from which you choose. That simply doesn't work here. There are too many edge cases and specifics that make any approach have holes in their coverage. There can be no catch-all here. There's where the idea of a privacy icon comes into play. The icon is well-defined and can replace with company-specific info. The purpose is to cut through the complexity. The problem is that it's used by companies, and companies necessarily cover everything. It's time-consuming and high impossible.

Here's the solution. Create a set of easily understood Privacy icons that "bolt on to" a policy. When you add a Privacy icon to your privacy policy it says the equivalent of "No matter what the rest of this privacy policy says, the following is true and preempts any conflict in this document...". The Privacy icon makes an iron-clad guarantee about some portion of how a company treats your data. For example, if a privacy policy includes the icon for "None of your data is sold or shared with 3rd parties", then no matter what the privacy policy says in the small print, it gets preempted by the icon and the company is legally bound to never sharing or selling your data. Of course, the set of icons still needs to be decided (we'll be having a workshop on the 27th of January to help figure it out).
What attributes of privacy should people care about?
Do not penalize business as usual.
Creative Commons?
WASHING SYMBOLS

40°C
Washable up to 40°C.

40°C mild
Washable up to 40°C in very mild wash conditions.

Hand wash
Hand wash only.

Do not wash.

Do not use bleach.

DRY CLEANING

P
You can dry clean your garment - normal process.

Professional dry clean only - mild process.

Do not dry clean.

DRYING

Tumble dry at low heat setting.

Do not tumble dry.

IRONING

Hot iron.

Warm iron.

Cool iron.

Do not iron.
Irreducible Complexity
Binding Icons
Bad actors won’t play?
Logging in with an existing account

You are connected to Yahoo. They know you as Aza Raskin.

Connect automatically, without asking.

You are connected to Yahoo. They want to know more about you. You don’t have to tell them, but if you do you get a more rich experience.
Normative.
7 Things That Matter Most
Is your data used for secondary use? And is it shared with 3rd parties?
Is your data bartered?

YOUR DATA IS
BARTERED OR SOLD
Under what terms is your data shared with the government and with law enforcement?
Does the company take reasonable measures to protect your data in all phases of collection and storage.
Does the service give you control of your data?
Does the service use your data to build and save a profile for non-primary use?
Are ad networks being used and under what terms?
YOUR DATA IS USED FOR PURPOSES YOU DO NOT INTEND

YOUR DATA IS BARRERED OR SOLD

YOUR DATA IS GIVEN UP WITHOUT A SUBPOENA

YOU CANNOT DELETE YOUR DATA, BUT YOU CAN EXPORT IT

SITE CONTAINS 3RD PARTY ADS

SITE CONTAINS 3RD PARTY ADS, WHICH TRACK YOU ACROSS MANY WEBSITES

THIS SITE HAS A SECURITY RATING OF 2.5. DO NOT GIVE FINANCIAL INFORMATION.

SITE BUILDS A PROFILE OF YOU FROM A VARIETY OF SOURCES
THE STRAWMAN
Is a Creative Commons for Privacy Possible

The 7 Things That Matter Most In Privacy