P3P Guiding Principles

W3C NOTE 21-July-1998

This Version:
http://www.w3.org/TR/1998/NOTE-P3P10-principles-19980721

Latest Version:
http://www.w3.org/TR/NOTE-P3P10-principles

Previous Version:
http://www.w3.org/TR/1998/NOTE-P3P10-principles-19980710

Editor:
Lorrie Faith Cranor (AT&T Labs-Research) lorrie@research.att.com

Signatories:
[See below]

Copyright © 1998 W3C (MIT, INRIA, Keio), All Rights Reserved. W3C liability, trademark, document use and software licensing rules apply.

Status of This Document

This document is part of the Platform for Privacy Preferences Project Activity. This document describes the intent of P3P development and recommends guidelines regarding the responsible use of P3P technology. It is one section of the P3P Implementation Guide. Comments to the editor or endorsements are welcome.

The Platform for Privacy Preferences Project (P3P) has been designed to be flexible and support a diverse set of user preferences, public policies, service provider polices, and applications. This flexibility will provide opportunities for using P3P in a wide variety of innovative ways that its designers had not imagined. The P3P Guiding Principles were created in order to: express the intentions of the undersigned members of the P3P working groups when designing this technology and suggest how P3P can be used most effectively in order to maximize privacy and user confidence and trust on the Web. In keeping with our goal of flexibility, this document does not place requirements upon any party. Rather, it makes recommendations about 1) what should be done to be consistent with the intentions of the P3P designers and 2) how to maximize user confidence in P3P implementations and Web services. We invite organizations, individuals, policy-makers, and companies who use P3P to join us in supporting these
Information Privacy

P3P has been designed to promote privacy and trust on the Web by enabling service providers to disclose their information practices, and enabling individuals to make informed decisions about the collection and use of their personal information. P3P user agents work on behalf of individuals to reach agreements with service providers about the collection and use of personal information. Trust is built upon the mutual understanding that each party will respect the agreement reached.

Service providers should preserve trust and protect privacy by applying relevant laws and principles of data protection and privacy to their information practices. The following is a list of privacy principles and guidelines that helped inform the development of P3P and may be useful to those who use P3P:

- CDMA Code of Ethics & Standards of Practice: Protection of Personal Privacy
- 1981 Council of Europe Convention For the Protection of Individuals with Regard to Automatic Processing of Personal Data
- CSA--Q830-96 Model Code for the Protection of Personal Information
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- The DMA's Marketing Online Privacy Principles & Guidance and the The DMA's Ethical Business Practice Guidelines
- HEW Fair Information Principles
- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
- Online Privacy Alliance Guidelines for Online Privacy Policies

In addition, service providers and P3P implementers should recognize and address the special concerns surrounding children's privacy.

Notice and Communication

Service providers should provide timely and effective notices of their information practices, and user agents should provide effective tools for users to access these notices and make decisions based on them.

Service providers should:

- Communicate explicitly about data collection and use, identifying the purpose for which personal information is collected and the extent to which it may be shared.
- Use P3P proposals to communicate about all information they propose to collect through a Web
Prominently post clear, human-readable privacy policies.

User agents should:

- Provide mechanisms for displaying a service's information practices to users.
- Provide users an option that allows them to easily preview and agree to or reject each transfer of personal information that the user agent facilitates.
- Not be configured by default to transfer personal information to a service provider without the user's consent.
- Inform users about the privacy-related options offered by the user agent.

Choice and Control

Users should be given the ability to make meaningful choices about the collection, use, and disclosure of personal information. Users should retain control over their personal information and decide the conditions under which they will share it.

Service providers should:

- Limit their requests to information necessary for fulfilling the level of service desired by the user. This will reduce user frustration, increase trust, and enable relationships with many users, including those who may wish to have an anonymous, pseudonymous, customized, or personalized relationship with the service.
- Obtain informed consent prior to the collection and use of personal information.
- Provide information about the ability to review and if appropriate correct personal information.

User agents should:

- Include configuration tools that allow users to customize their preferences.
- Allow users to import and customize P3P preferences from trusted parties.
- Transfer personal information only to sites with which the user has reached an agreement authorizing such transfers or when authorized by the user.
- Present configuration options to users in a way that is neutral or biased towards privacy.
- Be usable without requiring the user to store user personal information as part of the installation or configuration process.

Fairness and Integrity

Service providers should treat users and their personal information with fairness and integrity. This is essential for protecting privacy and promoting trust.
Service providers should:

- Accurately represent their information practices in a clear and unambiguous manner -- never with the intention of misleading users.
- Use information only for the stated purpose and retain it only as long as necessary.
- Ensure that information is accurate, complete, and up-to-date.
- Disclose accountability and means for recourse.

User agents should:

- Act only on behalf of the user according to the preferences specified by the user.

Security

While P3P itself does not include security mechanisms, it is intended to be used in conjunction with security tools. Users' personal information should always be protected with reasonable security safeguards in keeping with the sensitivity of the information.

Service providers should:

- Protect users' personal information with reasonable security safeguards in keeping with the sensitivity of the information.
- Use appropriate trusted protocols for the secure transmission of data.

User agents should:

- Provide mechanisms for protecting the personal information that users store in their P3P data repositories.
- Use appropriate trusted protocols for the secure transmission of data.
- Warn users when an insecure transport mechanism is being used.

Definitions

The following definitions reflect the way these terms are used in this document.

**personal information** - Data relating to an identified or identifiable user that is transferred to a service under a P3P agreement or stored in a user's P3P data repository. Note, the term personal information in this document does not refer to information exchanged in the course of interactions inherent to the
preferences - A set of rules that determines what action(s) a user agent will take or allow when involved in an interaction or negotiation with a service. Users' P3P preferences should reflect their attitudes towards the use and disclosure of their personal information.

proposal - A series of P3P statements that describe the privacy-related terms (practices) under which a service proposes to interact with a user or user agent.

service provider - The person or organization that offers information, products, or services from a Web site, collects information, and is responsible for the representations made in a practice statement. Note, the term service provider in this document does not refer to Internet Service Providers (ISPs), except where ISPs also provide services from Web sites.

user - An individual (or group of individuals acting as a single entity) on whose behalf a service is accessed and for which personal data exists.

user agent - A program that acts on a user's behalf. The agent may act on preferences (rules) for a broad range of purposes, such as content filtering, trust decisions, or privacy. For P3P purposes, a user agent acts on a user's privacy preferences. Users may use different user agents at different times.

Signatories

- Azer Bestavros, Ph.D., Senior Lead Technologist, Bowne Internet Solutions
- Ann Cavoukian, Ph.D., Information and Privacy Commission Ontario Canada, Commissioner; Participant in P3P Vocabulary Harmonization Working Group
- Lorrie Faith Cranor, D.Sc., P3P Interest Group Co-Chair; AT&T Labs-Research
- Josef Dietl, W3C
- Daniel Jaye, CTO, Engage Technologies
- Marit Köhntopp, Privacy Commissioner of Land Schleswig-Holstein, Germany
- Tara Lemmey, Chairman, Narrowline; TrustE Board Member
- Dr. Steven Lucas, CIO, MatchLogic
- Massimo Marchiori, P3P editor; World Wide Web Consortium
- Dave Marvit, Internet Strategist, Fujitsu Labs
- Maclen Marvit, VP Engineering, Narrowline Inc.; Member P3P syntax working group
- Yossi Matias, PhD, Department of Computer Science, Tel Aviv University
- James S. Miller, PhD, MIT Lab for Computer Science
- Deirdre Mulligan, Staff Counsel Center for Democracy and Technology; Coordinator of the Internet Privacy Working Group; and, Participant in P3P Vocabulary Harmonization Working Group
Group

- Joseph Reagle, P3P Interest Group Co-Chair; Policy Analyst, W3C
- Drummond Reed, Co-Founder, Intermind
- Lawrence C. Stewart, Chief Scientist, Open Market, Inc.