

P3P AND PRIVACY:

An Update for the Privacy Community

by *

CENTER FOR
DEMOCRACY
&
TECHNOLOGY

Deirdre Mulligan
Ari Schwartz



Information and Privacy
Commissioner/Ontario

Ann Cavoukian PhD.
Michael Gurski

Tuesday, March 28, 2000

INTRODUCTION

The Platform for Privacy Practices (P3P) is not a panacea for privacy, but it does represent an important opportunity to make progress in building greater privacy protections in the Web experience of the average user.

P3P is simply a standard or specification currently under development at the World Wide Web Consortium (W3C). That specification, when implemented in Web sites and browsers, will bring a measure of ease and regularity to Web users wishing to decide when and under what circumstances to disclose personal information. The barrage of privacy issues that bedevil the Internet can be partially addressed with the widespread adoption of the P3P specifications. It offers an important opportunity to build greater technical support for privacy-informed Web users and supports a catalyst on the part of Web sites

seeking to incorporate privacy protections into the Web's infrastructure.

While the development process has progressed, companies and privacy advocates have attacked it from many sides for more than two years. For example, two Citibank employees issued a paper expressing a concern that P3P might "let ordinary users see, in full gory detail, how their personal information might be misused by less trusted or responsible web site operators. Such knowledge may cause users to resist giving out information altogether. Some individual business groups have done focus studies on users, and, though the results deserve further study, some concluded that most users would prefer to give out only information needed for the transaction and that they do not like the idea of someone monitoring their browsing behavior." [1] Meanwhile others, such as Karen Coyle, are concerned that P3P might oversimplify and quite possibly misrepresent "the

* CDT and the Office of IPC/Ontario are members of the P3P Policy outreach working group at the W3C. This paper represents only the viewpoints of the two organizations and is not an official document of the working group of the W3C.

[1] http://www.w3.org/P3P/Lee_Speyer.html

trust interaction, and always in favor of the web site that is asking for an individual's information.” [2] Still others, like Jason Catlett, have conducted a premature post-mortem, suggesting that P3P will never be adopted by the critical mass of Web sites necessary to have an impact. Or that, even if adopted, it would be nothing more than an attempt by industry to maximize the collection of consumer data over the Internet. [3]

These various, often contradictory, views of P3P are understandable for two reasons. First, some have over-hyped the standard, claiming that P3P will, on its own, fully address privacy concerns. Second, the development of the specifications has been a lengthy process during which the initial proposal has undergone significant and often confusing changes.

While these concerns have varying degrees of legitimacy, as privacy advocates involved in the P3P process, we have committed ourselves to supporting the development of P3P understanding its strengths and limitations. P3P needs a regulatory or policy context to help protect privacy, it cannot do this by itself. More importantly, it is not, and should not be viewed or trotted out as a reason to discourage regulatory or self-regulatory efforts to protect privacy. As we suggest in this paper, P3P is a means of enabling Web sites to regularize their privacy vocabulary and bring these privacy policies front and center for the Web user's consideration. In other words, we have chosen to work on P3P because we seek to promote greater transparency. In our opinion P3P does not protect privacy, in and of itself. It does, however, help create a framework

for informed choice on the part of consumers. Any efficacy that P3P has is dependent upon the substantive privacy rules established through other processes — be they a result of regulatory, self-regulatory or public pressure.

It is our hope that privacy rules continue to be debated and developed, as they traditionally have, through democratic publicly-accountable processes. Individuals and businesses hoping to protect privacy solely through the P3P specification would be wise to review the Fair Information Practice Principles. A quick read should convince even the most optimistic of P3P supporters that P3P is neither designed nor suited for addressing all critical elements of privacy protection. Similarly, individuals who criticize P3P or suggest abandonment should be careful what they wish for. We do not want specification and standard settings bodies determining public policy. W3C does not wish to become the forum for public policy debates. We don't want to cede the development of substantive policy to technical organizations. However, to the extent that we can work with the technical community to build platforms and standards that support our social policies surely we should pursue such opportunities.

Many criticisms have been made regarding the delays in bringing P3P to fruition. Specifications like P3P take time. From its inception P3P was envisioned as a specification with a social purpose. As participants, we believe that the P3P process has been deliberative and thoughtful. W3C and the P3P working groups have actively solicited comments from all interested parties. We have met with

[2] <http://www.kcoyle.net/p3p.html>

[3] <http://www.junkbusters.com/standards.html>

interested parties across the spectrum and across the globe. We have sought out and engaged critics on all sides. We believe that doing so is critical to P3P's success, and will continue to do so. This outreach has taken time and effort. Everyone has his or her own agenda and perspective that can be misinterpreted as unnecessarily delaying the process. As advocates we continue to push for the timely finalization of the specification and the future development of P3P.

Part of the task has been to build a common vision and move forward. The Guiding Principles behind P3P embody that vision. The specification is the expression of 'intent' that counts in the P3P process. The Guiding Principles attest to P3P as an effort at bringing Web site privacy policies to the foreground, and to help Web users make informed decisions regarding the disclosure of personal information. We are committed to ensuring that P3P implementations are true to this intent.

While the use of P3P for political purposes and the length of the development period must be monitored, in the end, our greatest concern is that a specification designed to promote greater transparency and support individual choice regarding privacy may die before a single implementation comes to market.

This paper explains where P3P is in development and is a call to all who would like to see privacy on the Internet grow to:

- become directly involved and work to improve the current specification,
- vigilantly watch implementations,
- and, assuming that all goes well, ultimately support P3P's final recommendation to the W3C.

WHAT IS P3P 1.0?

Today, P3P is a sleeker, simpler specification than initially proposed. The original P3P specification contained three integrated features: 1) a vocabulary and specification for making privacy statements; 2) a protocol for negotiations between the individual and the Web site over privacy statements; and 3) a standard for storing personal information and controlling its transfer pursuant to 1 & 2. Combined, these features provided an overall framework for automating privacy decisions for Web users and Web sites and transferring personal information. These features were discussed and debated for over 2 years. In the mean time products emerged to help consumers store and manage their personal information. The P3P specification group decided to eliminate the data transfer and negotiation components of the specification and focus on the part of the specifications needed for Web sites to make machine readable privacy statements and deploy client side tools to decipher them for consumers.

P3P 1.0 creates the framework for standardized, machine-readable privacy policies, and consumer products that read these policies. Like all specifications many critical decisions are in the hands of developers. However, the Guiding Principles that inform both the development and use of P3P tools directs builders and users on issues that the P3P working group felt were critical to the soundness of P3P and its purpose. Within the confines of the specification and the Guiding Principles, P3P allows innovation. We hope that tools that read and compare privacy policies as directed by consumers will come to the market. Eventually we hope that other features — such as a way to verify and repudiate policies — can be added to the specification, but for now

the purpose of P3P is simply to advance transparency by making notices machine readable.

P3P is in “Last Call” at the W3C with an open invitation at their Web site to comment. Many concerns and suggestions have already been shared. For these we are very grateful. But we need more comments, suggestions and criticisms. The specification is in last call to the end of April, the public still has a chance to comment while implementations are being developed. When this period ends and a few successful implementations have been created, the W3C will vote on recommending it as a Web standard: P3P 1.0. Therefore, there is still time to improve the specification and monitor the implementations as they are created. Details about the public comment period conclude this paper. [4]

HOW P3P 1.0 WILL HELP PROTECT PRIVACY

P3P can help standardize privacy notices

On a P3P 1.0 enabled Web, all privacy policies will have the same basic machine-readable fields that will express a company’s privacy practices. While this does not offer privacy protection, if implemented, it could greatly advance transparency and be used to support efforts to improve privacy protection. As stated above, it does not address the full range of privacy considerations. But, it is designed to facilitate the exchange of information about privacy policies in a fashion that maps on to the Internet. P3P does not preclude the use of other technical or legal means of protecting privacy. In fact, the working group has sought input

from both builders of privacy enhancing tools and those responsible for implementing and enforcing privacy laws. P3P is just one stone in the foundation. It needs to be used in concert with effective legislation, strategic policy and other privacy enhancing tools. For example:

1. Countries with data protection and privacy laws and others seeking to police compliance with privacy standards could find the automated ability to assess a businesses’ privacy statement useful in their broader oversight and compliance program. — Searching and gathering privacy policies could be simplified through P3P. P3P would allow the policies to be collected and analyzed in a standard machine-readable format. Governments and organizations would be able to simply search through P3P statements to find companies whose notice does not meet privacy standards in various areas. In the current version of P3P, companies could even point to regulatorybodies that oversee them to help route privacy complaints.

2. Users could more easily read privacy statements before entering Web sites. — Today, it is often difficult to find privacy notices. Once found, they are frequently written in complicated legalese. P3P implementations could allow users to assess privacy statements prior to visiting a site, and allow users to screen and search for sites that offer certain privacy protections.

3. Cutting through the legalese — A company’s P3P statement cannot use difficult to understand or unclear language. The standardization and simplification of privacy assertions into statements that can be automated will allow users to have a clear sense of who does what with their information.

[4] W3C members who would like to become more actively involved can join the P3P working groups. Organizations and companies can join the W3C specifically to work on P3P.

4. Enterprising companies or individuals could develop more accurate means of rating and blocking sites that do not meet certain privacy standards or allow individuals to set these standards for themselves. Several companies already rate and block Web sites that do not meet certain privacy standards. Today, creating the tools and knowledge that support these products is difficult and time consuming. By providing an open standard, P3P 1.0 could enhance the transparency, accuracy and detail of existing products, and could encourage an influx of new privacy enhancing products and services.

P3P can support the growth of more privacy choices, including anonymity and pseudonymity

Full anonymity is an important protection for privacy on the Internet. The ability to use the Internet with a pseudonym is also critical. These options must be supported and promoted. However, with anonymity or pseudonymity a person would be hard pressed to be involved in the full diversity of interactions occurring on the Internet. For privacy to be part of the Internet infrastructure, we must deploy tools that assist individuals in controlling personal information when they choose to, or need to, disclose it. P3P 1.0 can be used with anonymity tools to allow users to have more control over their personal information. A user should be able to be anonymous in one context and identifiable in another. The ability to have Web sites' privacy notices parsed and interpreted by a privacy tool can assist individuals decision-making regarding when and to whom to disclose personal information. Today, reading policies is a time consuming, cumbersome and sometimes impossible task. P3P 1.0 would help change that.

WHAT P3P WILL NOT DO:

P3P cannot protect the privacy of users in jurisdictions with insufficient data privacy laws

The W3C is a specification setting organization; it does not have the ability to create public policy nor can it demand that its specifications be followed in the marketplace. While different members of the W3C may have different reasons for engaging in the process nothing in the P3P Specification or the P3P Guiding Principles presumes that P3P is designed to replace public policy or a public policy process. Accordingly, P3P is designed to allow for statements about data practices, which are in turn directed by law, regulatory procedures, self-regulation or other forces.

We believe that better data privacy laws and further self-regulatory efforts are necessary to protect consumer privacy internationally. As privacy advocates, we believe that — armed with more information — individuals will seek out companies that afford better privacy protection. Recent consumer pressure on companies that collect personal information like there is no tomorrow, show that the public will act to protect their privacy if given simple, practical tools and advice to aid them. It also shows that companies can be made to moderate or reverse their policies and practices, if only temporarily. P3P can and should be used in concert with public policy to help protect privacy.

P3P cannot ensure that companies follow privacy policies

If a company says that they are going to do one thing and does something else, no technological process can stop them. Deception must be stopped through public policy processes, legislation and

the courts. Even in the United States, a country with limited consumer privacy protections, the Federal Trade Commission has brought cases against companies that do not follow posted privacy policies.

P3P would make privacy policies transparent. It does not ensure that the policies are followed. No technological process can ensure that companies comply with law or statements they choose to make. But, P3P will lead to greater openness, more informed Web users and therefore greater accountability.

WHY DO WE SUPPORT THE DEVELOPMENT OF P3P?

Even the best possible P3P1.0 implementation will not bring instant privacy protection to the Web. But it will bring clear progress. It will also inform the privacy debate by providing focus on Web sites and their privacy policies

Suffice it to say that establishing the technical terms for a social protocol is a complicated matter. P3P, in attempting to provide an automatic, common Web language to describe the collection and use of personal information, has been grappling to find a way to do just that. Much work remains to be done. Many members of the computer industry believe that P3P will increase consumer trust. They have donated time and effort to P3P. The Center for Democracy and Technology and the Office of Information and Privacy Commissioner/Ontario — along with other international privacy advocates, such as Joel Reidenberg of Fordham University and Marit Kohntopp of the Office of the Privacy Commissioner Schleswig-Holstein — have chosen

to commit resources to P3P because we believe it is a component of improved privacy practices on the Internet. We intend to ensure that privacy remains the top priority in the drafting of the P3P specification and the deployment of products built upon it.

If, after the P3P vocabulary is completely stable, there few or poor implementations, we will step back from P3P. However, we will do so with the knowledge that P3P's failure was not from our lack of effort.

Even with P3P, countries with lesser protections must strengthen their Laws. Yet standardized machine-readable privacy policies will still be an important tool for Internet users. With a little commitment and leadership from the privacy community, we can make P3P a step towards building privacy into the global Web architecture.

We encourage you to join us as we move forward. To do so, simply read the most recent version of the specification at: <http://www.w3.org/TR/P3P/> and send your comments to: www-p3p-public-comments@w3.org