The Role of Privacy Advocates and Data Protection Authorities in the Design and Deployment of the Platform for Privacy Preferences

Lorrie Faith Cranor

http://lorrie.cranor.org/

The Platform for Privacy Preferences (P3P) project [1] provides a standard way for web sites to communicate about their data practices. Developed by the World Wide Web Consortium (W3C) [2], P3P includes a machine-readable privacy policy syntax as well as a simple protocol that web browsers and other user agent tools can use to fetch P3P privacy policies automatically. P3P-enabled browsers can allow users to do selective cookie blocking based on site privacy policies, as well as to get a quick "snap shot" of a site's privacy policies.

The P3P specification includes a standard vocabulary for describing a web site's data practices, a set of base data elements that web sites can refer to in their P3P privacy policies, and a protocol for requesting and transmitting web site privacy policies. P3P policies are encoded in a machine-readable XML format using the P3P vocabulary. The P3P protocol is a simple extension to the HTTP protocol used for fetching web pages. P3P user agents use standard HTTP requests to fetch a P3P policy reference file from a well-known location on the web site to which a user is making a request. The policy reference file indicates the location of the P3P policy file that applies to each part of the web site. There might be one policy for the entire site, or several different policies that each cover a different part of the site. The user agent can then fetch the appropriate policy, parse it, and take action according to the user's preferences.

In this paper I discuss how P3P was developed and the role that privacy advocates and data protection authorities played in its development. I will also discuss the role that privacy advocates and data protection authorities might play in the future of P3P and other Internet standards efforts [3].

The Development of P3P

In 1995, members of the Platform for Internet Content Selection (PICS) [4] working groups at W3C began discussing the possibility of using PICS as a tool to help Internet users protect their privacy. PICS is a system for labeling web content according to a set of criteria called a rating system. While PICS ratings systems could be used to capture virtually any type of information about web content, PICS was being applied mostly to rate web pages according to their suitability for children. Indeed the PICS effort had been launched primarily as a non-legislative alternative to the U.S. Communications Decency Act and other similar legislation. But, as PICS co-chair Paul Resnick suggested at the June 1996 Federal Trade Commission Workshop on Consumer Privacy on the Global Information Infrastructure [5], PICS could also be used to rate web sites according to their information practices. Fordham University Law Professor Joel Reidenberg wrote a PICS rating system based on the Canadian Standards Association privacy standard to demonstrate this idea. Resnick also proposed that PICS be extended to allow people to negotiate with web sites over information practices. There was much enthusiasm for this idea at the workshop, although some of the privacy advocates present warned that the model would need to be supplemented by enforcement mechanisms and laws. So in the fall of 1996 the PICS co-chairs worked with the Center for Democracy and Technology (CDT) to gather industry support for pursuing this idea.

In mid November 1996, CDT convened the Internet Privacy Working Group (IPWG) to further explore the development of a PICS-like privacy tool. Initial participants included representatives from AT&T, IBM, America Online, Microsoft, the Electronic Frontier Foundation, DMA, W3C and others. The group appointed a "vocabulary subcommittee" to develop a draft privacy vocabulary that web sites could use to describe their privacy practices. The subcommittee produced several drafts of a privacy vocabulary and worked with W3C to develop a demonstration privacy tool [6] for the June 1997 FTC privacy workshop. P3P was introduced outside the US in the spring of 1997 at a Paris meeting of representatives from data protection authorities.

While P3P was focused on negotiating agreements about web site privacy practices, if was often suggested that P3P should also include mechanisms for transferring data according to these agreements. There was growing interest in tools that would allow users to fill out online forms automatically, and some IPWG members felt that P3P should include these tools as well so that all data transfer would be done under P3P control. On the other hand, other IPWG members were reluctant to associate a privacy protection tool with a tool that made data transfer easier. No consensus on this issue was ever reached within IPWG. However, W3C management later decided that data transfer mechanisms should be included as part of P3P. Two years later the P3P Specification working group removed the data transfer mechanism for a combination of policy and technical reasons.

In May 1997, P3P was launched officially as a W3C project. Over the next four years, a series of working groups were convened by W3C. These working groups were composed of representatives from some of the W3C member companies and organizations, as well as invited experts from academia and government. The overall P3P model stayed pretty much the same during this period; however, the specific details changed regularly. The P3P vocabulary evolved. Cookie-like persistent identifiers were added and later removed. And the data transfer mechanism was redesigned several times before it was finally dropped [7]. The biggest change was removing the concept of negotiation and agreement from P3P, focusing instead on providing a standard format for notice about web site privacy practices.

The use of the term "negotiation" within P3P evolved throughout the project. Originally many of

the participants envisioned a system that would allow web sites and user agents to haggle over privacy practices, engaging in a series of offers and counter offers. This multi-round negotiation was later replaced with a single-round negotiation in which the site has to make all of its offers up front. If more than one offer is made, the user agent may choose which one to accept. Eventually negotiation was removed altogether in order to simplify P3P implementation and make it possible for web sites to implement P3P without adding any special software to their servers. Existing servers could be configured to advertise the location of their P3P policies, and user agents could fetch these policies using standard web protocols. Furthermore, without the requirement that they attempt to negotiate an agreement, user agent tools could simply present privacy information to a user in an easy-to-understand format, without necessarily evaluating it or using it to make decisions.

As the P3P specification evolved, public working drafts were issued every few months. The P3P working groups solicited feedback on these drafts from W3C members and the public. Official responses were given to all substantive comments submitted.

Software developers at several companies and universities began to build P3P user agents and editors based on early drafts of the P3P specification. In addition, about 100 companies and organizations P3P-enabled their web sites in 2000 and 2001. As people used the specification, they raised a number of concerns. The Specification working group addressed some of these concerns by adding clarifying language to the specification; other concerns were addressed with changes to the P3P vocabulary and protocol.

The first major commercial user agent implementation of P3P appeared in the Microsoft Internet Explorer web browser in the summer of 2001 [8]. IE6 can filter cookies based on P3P policies. It also allows users to request a privacy report generated from web site P3P policies.

In February 2002, AT&T released a public beta of a P3P user agent add-on for the Internet Explorer web browser. Called the AT&T Privacy Bird [9], this tool checks for P3P policies at every web site a user visits. It displays a green bird icon at sites that match the user's privacy preferences, a red bird icon at sites that do not match, and a yellow bird icon at sites that have no P3P policies. Users can click on the bird to get more detailed information about the site's privacy policy, including a link to the full human-readable policy, a link to the site's opt-in or opt-out page, and a list of ads and other content embedded in the site that may have their own privacy policies.

IBM released a P3P policy editor tool that web sites can use to create their P3P policies [10]. This tool has been used by many of the web sites that have adopted P3P.

The W3C created outreach groups in both North America and Europe to work towards widespread P3P deployment. The North American group is working closely with the Internet Education Foundation and focusing on getting P3P deployed at the top 100 web sites. Already P3P is deployed at a number of major companies including AT&T, Microsoft, IBM, and Procter and Gamble. It is also being used by DoubleClick and some of the other major online advertising networks. And it is being used by Yahoo, Lycos, About.com, several US Congressional web sites, and a wide range of other web sites. The North American group created p3ptoolbox.org to provide a centralized online resource for getting information about using P3P.

In January 2002 the P3P Specification working group released a stable "Proposed Recommendation" draft of the P3P specification [11]. This draft was the result of over five years of work and took into account the suggestions of many individuals who had commented on earlier public drafts. A final

P3P 1.0 “Recommendation” is expected in Spring 2002 after the W3C members review and vote on the Proposed Recommendation.

Participation of Privacy Advocates and Data Protection Authorities

Throughout the P3P design process, data protection authorities and privacy advocates played an important role. Representatives from several data protection authorities joined P3P working groups or attended working group meetings and participated in the process directly. These included representatives from the French CNIL, the Ontario Information and Privacy Commission, the Privacy Commissioner of Schleswig-Holstein, and the Hong Kong Privacy Commissioner’s Office. In addition, several experts from academia as well as representatives from CDT and TRUSTe participated in the development of P3P. While many of the other working group members were official representatives of the companies that employed them, most considered themselves to be privacy advocates as well. These individuals often rejected proposed solutions that would have served to benefit their companies if they personally believed that they were not consistent with the interest of protecting privacy. While these individuals were accountable to their employers, most of them did not consult with their employers on every decision that had to be made, and many of them indicated frequently that their comments represented their personal opinions.

In January 1998 the European Commission DG XV issued an opinion on P3P [12]. In this opinion it was suggested that the P3P vocabulary be expanded to include information about remedies should web sites fail to comply with their stated privacy policies. This suggestion was taken into consideration and a disputes section with a remedies subsection was added to the P3P vocabulary. The opinion also raised concerns about how defaults would be set in P3P user agents as well as whether these agents might transfer data to web sites without user consent. The decision to remove the concept of automatic data transfer from P3P reduced this concern somewhat; however, the choices implementers make about defaults remain very important.

In September 1999 the Article 29 Working Party, representatives of the European Commission, and representatives from the P3P working groups met in Brussels to discuss options for using P3P to comply with the European Union Data Protection Directive. The meeting was a very good opportunity for the Working Party members to learn more about P3P, and for the P3P working group members to better understand some of the concerns that had been raised from the perspective of compliance with the European Directive. The meeting was supposed to result in a formal joint report and in follow-up discussions. Unfortunately this did not happen due to logistical problems. However, the P3P working group members who attended the meeting did take the European concerns back to the working group, and discussions continued informally. As the vocabulary continued to evolve, I believe many of the issues raised at the Brussels meeting were taken into account.

In August 2000 representatives from the P3P working groups gave presentations at the privacy summer school in Kiel. Following the presentations the Privacy Protection Commissioners of Berlin, Brandenburg, Hamburg, Northrhine-Westphalia, Schleswig-Holstein and Zurich held a press conference and issued a statement [13]:

> ... P3P technology is useful for online privacy, but not sufficient on its own because P3P only offers a basic standard for privacy protection. Under any circumstances, additional, effective privacy monitoring and precise laws in order to protect Internet users are required. P3P allows to transfer a great part of the model European privacy protection acts into “bits and bytes”. It is

more difficult for privacy protection in the USA where citizens have to get by without the backing of laws and Privacy Protection Commissioners.

In Germany P3P has to be implemented as soon as possible and on its basis a comprehensive privacy concept has to be developed in order to adequately realize the Teleservices Data Protection Act. P3P 1.0 is a first step in the right direction. With P3P 1.0 the development in this area has not yet come to an end, but additional features have to be integrated. In the long run the use of P3P and other privacy tools could be an advantage in market competition for German Internet business, as the Teleservices Data Protection Act incorporates a high degree of privacy protection in Europe-wide comparison. According to surveys from many countries, customers will prefer websites where a maximum of privacy protection is technically guaranteed.

P3P is an important building block of a new privacy protection concept that increasingly focuses on transparency and market-economic elements. P3P provides the Privacy Protection Commissioners new possibilities for co-operation with the industry and to make effective privacy protection in Europe a competitive factor. In the future consumers should be given more and more the possibility to create demand for privacy protection through their consumer behaviour. This should make it clear to the companies that the European privacy protection is a locational advantage and that privacy-invasive sites don't have a chance in the market in the long run.

Since the Kiel meeting, representatives from Schleswig-Holstein have continued to be actively involved in the P3P working groups, and were very helpful as we ironed out some of the last remaining vocabulary issues. While I believe that most of the participants in the P3P working groups really are working towards similar goals of helping consumers better protect their privacy, there are some fundamental differences in understanding about what will best lead us towards these goals. One area that proved particularly difficult was the discussion of what constitutes "personally identifiable data," "identifiable data," or "identified" data. While it is quite clear that some data such as name, address, or telephone number is identifiable, data such as IP address is less clear. In some parts of the P3P specification distinctions were made between data that could be used to identify a person and data that actually is used to identify a person. This raises questions about what we mean by could — just that something is theoretically possible, or must it be reasonably possible to actually do it? And are we concerned about the data being used by another party other than the data collector (for example law enforcement) to identify someone, or are we only concerned about its use by the data collector? Throughout this discussion many of the American working group members actually thought that a fairly strict interpretation of identifiable would be needed, but the data protection authority representatives argued for an interpretation based on the idea of "reasonable" and focusing on what would be possible for data collectors to do on their own. In the end we removed the term "personally identifiable data" from the specification and adopted the term "identified data" to mean "Data that reasonably can be used by the data collector to identify an individual."

I believe that the participation of representatives from the data protection authorities helped us to improve the P3P vocabulary and also helped us think about how P3P might be used to complement data protection laws. While the proceedings of the P3P working group take place in English and the P3P working group conference calls are held at times that may not be as convenient outside the US as they are in the US, we were able to get valuable input from data protection authority representatives outside the United States. We also had active participation from the Ontario Commission, which did not have problems with language or time zones. The appointment of a European W3C staff member to work

with the P3P working group was also helpful.

I think procedure more than language or time zones proved to be a handicap in the participation of data protection authority representatives in the development of P3P. Government agencies and international working parties tend to have formal procedures they have to follow before they can send representatives to meetings or offer official comments. However, Internet standards are developed at a rapid pace, and there is often not enough time for official procedures to be followed and comments submitted before a new draft is available that may make comments on the previous draft obsolete. As much as it seems silly to suggest that a standard that has been five years in the making is proceeding on rapid "Internet time," the evolution of P3P has indeed occurred on Internet time. Most of the work of the working groups has taken place via email, and we hold weekly conference calls in which new issues get resolved almost every week. While most of these issues are relatively minor details, it is the collection of these details that will determine the ability of P3P to be an effective standard. Often when a new issue was raised in the P3P working group we scrambled to get feedback from a diverse group of viewpoints before the next meeting so we could determine whether there were any aspects of the decision that might have implications not readily apparent. It was easy to get quick unofficial feedback from some of our academic colleagues and from those data protection authorities who had representatives monitoring the working group mailing list and participating in conference calls. But getting even unofficial feedback from those not up to speed on the details of the specification was difficult. And even if they were up to speed, some were reluctant to provide unofficial feedback and wished to wait for the opportunity to provide official comments.

Throughout the P3P development process a number of US privacy advocates and interest groups have been highly critical of P3P. While the P3P working groups were able to make changes to the P3P specification to address some of the specific criticism, one major substantive criticism remains. Some privacy advocates disagree with the entire premise of P3P — they do not believe that by making it easier for consumers to access and understand web site privacy policies that the general state of data privacy will begin to improve. Some argue that P3P could even have the opposite effect, because they believe the existence of P3P may serve to stall proposed privacy legislation. Much has been written by those on both sides of this debate [14, 15, 16, 17].

Despite the apparent dichotomy, I think both P3P supporters and critics generally agree that a many-pronged approach is needed to improve privacy protections. I think the major differences between the sides have to do with disagreements about the most productive approaches and best use of resources. I think the disagreements became somewhat exaggerated, in part, due to a feeling among some privacy advocates that they could not influence the development of P3P unless they unconditionally supported it. This in turn may have been due in part to the way the P3P work was structured at the W3C. Individuals not affiliated with W3C member companies and organizations could participate in W3C working groups as "invited experts," but such participation was time intensive and required these individuals to abide by W3C member confidentiality rules. While frequent public working drafts were published and comments invited, non-members never had the opportunity to provide input on the overall goals of the project. Indeed, even the working group members themselves never developed a formal requirements document for the project. Such a document would have been useful both for focusing the development process as well as a way of vetting the concept of P3P publicly and getting buy-in (or understanding its shortcomings) early in the process [18].

Some privacy advocates who were not members of the P3P working groups did participate productively in the development of P3P by submitting comments on the P3P working drafts. This did

include some privacy advocates who do not consider themselves to be P3P supporters, but none-the-less contributed constructive criticism. A more open specification development process might have led to more participation along these lines.

The Future

In the future I hope we can find ways to use both official and unofficial channels to get more rapid feedback on proposed changes to the P3P specification. If data protection authorities are to play a meaningful role in future Internet standards efforts, I think they will need to find ways to work on Internet time, even if it means using unofficial channels. There were a number of instances when we were able to make very effective use of unofficial channels in the P3P effort. A number of frank personal conversations with representatives of data protection authorities helped me understand perspectives that could not be stated officially in a timely fashion or in some cases at all.

In addition, I think in order for data protection authorities and non-profit advocacy organizations to participate meaningfully in Internet standards efforts, they need to be able to devote enough resources to follow these efforts. It is helpful to have someone who is both technically proficient and understands policy issues available to read the correspondence on the working group mailing lists and participate in discussions. This is a problem not just for data protection authorities, but also for the non-profit organizations that have tried to participate in P3P as well as other Internet standards efforts. CDT and IEF managed to participate in the P3P process quite effectively, but they have done this by designating one or two staff members who have spent a large percentage of their time working on P3P. In addition, CDT recently launched a project with the goal of finding ways to support the participation of public interest organizations in Internet standards efforts [19].

Returning to P3P specifically, the main work left to do is to get P3P deployed. Data protection authorities can assist in this by encouraging web sites under their jurisdiction to use P3P. Authorities may wish to distribute information about using P3P, provide examples of exemplary P3P policies, or translate instructions for P3P enabling web sites into languages appropriate for the people in their jurisdiction. Authorities may also consider allowing sites to submit their P3P policies rather than filling out separate forms as part of their own compliance procedures. They might develop automated tools that can extract some of the necessary information directly from the P3P policies.

Both data protection authorities and public interest groups can play a significant role with respect to P3P is in the development of default settings and other aspects of the user interface of P3P user agents. A lot of concerns have been raised about the P3P user interface, and especially about default settings, but very few concrete suggestions have been made as to what the interface should look like or what the default settings should be. I realize that it is somewhat difficult to make such recommendations while P3P is still an abstract concept and it is difficult to understand what the range of possibilities might be. But now that P3P user agents are emerging, it is time for data protection authorities and public interest groups to review them and to make specific suggestions about how they might be improved. They might take these suggestions to the companies who have already implemented P3P user agents, or they might fund projects to develop P3P user agents built especially to meet these needs. In addition, most P3P user agents come equipped with an ability to import settings files. Data protection authorities and public interest groups might consider developing recommended setting files for these user agents and distributing them on their web sites.

With P3P 1.0 well on its way, discussions have begun informally about developing a P3P version

2. It is likely that W3C will solicit formal input about this from both W3C members and the public before the end of the year. It is important that privacy advocates and data protection authorities get involved in these discussions to determine whether a version 2 is needed, and if so, what its goals should be.

1. http://www.w3.org/P3P/
2. http://www.w3.org/
3. I serve as chair of the P3P Specification Working Group; however, the opinions expressed here are my personal opinions, and do not necessarily reflect Working Group consensus or official W3C policy.
4. http://www.w3.org/PICS/
5. Workshop on Consumer Privacy on the Global Information Infrastructure. http://www.ftc.gov/bcp/privacy/wkshp96/privacy.htm
6. FTC Comment: Script of W3C P3 Prototype. http://www.w3.org/Talks/970612-ftc/ftc-sub.html
7. Removing Data Transfer from P3P. http://www.w3.org/P3P/data-transfer.html
8. Privacy in Internet Explorer 6 by Aaron Goldfeder and Lisa Leibfried http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnpriv/html/ie6privacyfeature.asp.
9. http://privacybird.com/
10. http://www.alphaworks.ibm.com/tech/p3peditor
11. The Proposed Recommendation is available from http://www.w3.org/TR/2002/PR-P3P-20020128/. The most recent version of the P3P Specification is available from http://www.w3.org/TR/P3P.
12. European Commission Working Party on the Protection of Individuals with regard to the processing of Personal Data. Opinion 1/98. Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS). http://www.epic.org/privacy/internet/ec-p3p.html
13. Independent Centre for Privacy Protection Schleswig-Holstein. 29 August 2000. Press Release: New Standard in Online Privacy presented in Germany. http://www.rewi.hu-berlin.de/Datenschutz/DSB/SH/somak/somak00/p3pe_pm.htm
14. Lorrie Faith Cranor. Agents of Choice: Tools that Facilitate Notice and Choice about Web Site Data Practices. Proceedings of the 21st International Conference on Privacy and Personal Data Protection, 13-15 September 1999, Hong Kong SAR, China, p. 19-25. http://lorrie.cranor.org/pubs/hk.pdf
15. Deirdre Mulligan, Ari Schwartz, Ann Cavoukian, and Michael Gurski. P3P and Privacy: An Update for the Privacy Community. March 2000. http://www.cdt.org/privacy/pet/p3pprivacy.shtml
16. Karen Coyle. A Response to “P3P and Privacy: An Update for the Privacy Community.” May 2000. http://www.kcoyle.net/response.html
17. Electronic Privacy Information Center and Junkbusters. Pretty Poor Privacy: An Assessment of P3P and Internet Privacy. June 2000. http://www.epic.org/reports/prettypoorprivacy.html
18. The official W3C process rules as well as actual working group practice have evolved considerably since the P3P project was launched in 1997. Today most working groups begin their work by developing requirements documents, and many working groups are being chartered with public mailing lists and no requirement that working group proceedings are member confidential.
19. The Internet Standards, Technology & Policy Project: Internet Technology in the Public Interest. http://www.cdt.org/standards/overview.shtml