The Platform for Privacy Preference as a Social Protocol: An Examination Within the U.S. Policy Context

HARRY HOCHHEISER
University of Maryland, College Park

As a "social protocol" aimed at providing a technological means to address concerns over Internet privacy, the Platform for Privacy Preferences (P3P) has been controversial since its announcement in 1997. In the U.S., critics have decried P3P as an industry attempt to avoid meaningful privacy legislation, while developers have portrayed the proposal as a tool for helping users make informed decisions about the impact of their Web surfing choices. This dispute touches upon the privacy model underlying P3P, the U.S. political context regarding privacy, and the technical components of the protocol. This article presents an examination of these factors, with an eye towards distilling lessons for developers of future social protocols.

Categories and Subject Descriptors: K.4.1 [**Computers and Society**]: Public Policy Issues—*Privacy*; *regulation*; K.5.2 [**Legal Aspects of Computing**]: Governmental Issues—*Regulation*; K.1 [**The Computer Industry**]: *Standards*; C.2.2 [**Computer-Communication Networks**]: Network Protocols—*Applications*

General Terms: Human Factors, Legal Aspects, Standardization

Additional Key Words and Phrases: Privacy, social protocols, P3P

1. INTRODUCTION

> "Microsoft Corp., in a bid to help the Internet industry ward off new privacy laws from Congress, is touting a suite of tools it has built into the next version of the company's Internet browser, which will allow more control over how much personal information Web sites can collect." *Washington Post*, March 29, 2001 [Walker 2001]

Microsoft's Spring 2001 announcement of Internet Explorer 6.0 (IE 6.0) was a notable step in the ongoing debate over Internet privacy. As reported in the Washington Post, IE 6.0 includes a "privacy thermostat" that could be used to control the use of Web cookies [Walker 2001]. This in itself was not novel: "cookie-cutter" and related programs had been available for some time. IE 6.0

Authors' address: Human-Computer, Interaction Laboratory, A. V. Williams Bldg., 3174, College Park, MD 20742; email: hsh@cs.umd.edu.

is different in that it uses the Platform for Privacy Preferences (P3P) to provide this capability. Developed by the World Wide Web Consortium (W3C), P3P is a tool designed to inform users about the privacy practices of a Web site, so that they might decide whether or not to interact further with that site.

This announcement—or, at least, its press coverage—was also notable for the direct tie between Microsoft's announcement and efforts to avoid federal Internet privacy legislation in the United States. Since U.S. Department of Commerce discussions in 1995 established the model of industry self-regulation as the government's preferred approach to the protection of Internet privacy [National Telecommunications and Information Administration 1995], a variety of legislative measures aimed at Internet privacy protection have been proposed. These proposals have generally faced stiff opposition from legislators favoring self-regulatory approaches. P3P is the the most visible attempt to develop self-regulatory technological measures to protect privacy. As the first major Web browser to include P3P support, IE 6.0 was a milestone in the development of P3P, a process that the W3C initiated in 1997.

The history of P3P has been controversial. Many privacy advocates have questioned the motives behind P3P, arguing that its development has been championed by corporations more interested in avoiding legislation than in protecting privacy. They have also criticized the pace of development and contents of the protocol. P3P developers and supporters have argued that privacy is a complex problem with multiple, competing interests. In their view, the long development time has been a legitimate and appropriate result of their efforts to listen to outside criticism and commentary. Microsoft's inclusion of P3P functionality in IE 6.0 can be seen as the culmination of almost four year's work towards the development of technological tools for privacy self-regulation, or it could be seen as the latest in a series of cynical attempts to use technological smoke and mirrors to avoid privacy legislation.

The advocates and critics of P3P are both partially correct: P3P is a well-intentioned effort to build effective privacy protection tools, and an effective tool in the argument for self-regulation as opposed to legislation. This seeming contradiction is largely a function of P3P's specificity. As a narrowly-defined tool aimed at addressing the specific goal of helping users make informed decisions about the privacy implications of their Web browsing decisions, P3P does not claim to provide a comprehensive solution to all Internet privacy dilemmas.

P3P is perhaps the most recent example of a new class of technical measures aimed at addressing policy issues. These technical measures—referred to as "social protocols" [Cranor and Reagle 1998]—often define the intersection between technology and policy. In attempting to address existing social and political concerns, these protocols are more than technical proposals. They can change the terms of the debate and influence policy discussions.

The history of P3P shows that the development of social protocols requires consideration of social, political, and other issues that are traditionally outside the scope of technical development efforts. P3P has been used as a rhetorical device by both supporters and opponents, its capabilities have been oversold, and technical discussions have been inextricably linked to political

debates over the nature of privacy. These difficulties may be an unavoidable by-product of any attempt to use technology to address controversial social problems.

This article will use an examination of P3P from both historical and technical perspectives to build an understanding of the controversies behind P3P and its implications for developers of future social protocols. This analysis will focus on the political, legislative, and regulatory context in the U.S. Discussions of the role of P3P in Europe, Canada, Australia, and elsewhere are largely beyond the scope of this work.

2. WHAT IS P3P?

P3P is a protocol for automating the transfer of privacy policies between Web sites and Web browsers, and the comparison of those policies with statements of user preferences. P3P's developers argue that this mechanization will reduce confusion and streamline the often difficult and uninformative process of retrieving and interpreting privacy policies, thus helping users make more informed choices about the privacy implications of their Web-surfing actions [Reagle and Cranor 1999].

To be P3P-compliant, a Web site operator must generate a machine-readable version of their privacy policy. The P3P specification uses the Extensible Markup Language (XML) to define a vocabulary regarding information practices. This vocabulary contains terms that can be used to describe the information that will be collected by the site; what the information will be used for; whether or not the users will be able to access or change the information; how long it will be stored; who is responsible for the Web site; and other related details [Cranor et al. 2002a] (see Figure 1 for a summary of key elements of the P3P vocabulary and Figure 2 for a sample P3P privacy policy).

When a user of a P3P-compliant browser goes to a Web site, the browser's first action is to follow a specific protocol for requesting the site's privacy policy. The browser then uses the downloaded policy to inform the user about the privacy implications of visiting the site. Browser developers have wide latitude in the exact nature of this interaction. Some browsers will compare the contents of the privacy policy to a stored description of the user's privacy preferences and respond appropriately. If the behavior stated within the policy is consistent with the user's preferences, interaction with the site will continue without interruption. If the policy specifies behavior that does not match these preferences, the browser might present a dialog box to the user, explaining the potential conflict and presenting the user with the choice of canceling or continuing. Other browsers may simply update an icon or other passive display to alert the user of any possible conflict.

In addition to complete privacy policies (Figure 2), the P3P specification defines the notion of a compact policy that can be used to optimize performance, by reducing the time needed to retrieve a complete policy statement. A compact policy summarizes a full policy, replacing the complete XML statement with a series of short tokens that describe a subset of the practices described in a complete policy. Compact policies are limited to information about HTTP

ENTITY	The legal entity making the representation of the privacy practices. Includes the entity's legal name and contact information.	
ACCESS	The facilities (if any) that the site provides to allow users to access information that identifies them or to have questions addressed by the service provider. Possible values include "all" (access is given to all identifying data), "nonident" (the web sites does not collect identifying data, "none" (no access is provided), and three intermediate fields indicating varying levels of access to some subset of collected data.	
DISPUTES	Descriptions of procedures that might be followed in case of disputes over privacy practices. Use of this field is encouraged, but it is not required.	
STATEMENT	a delimiter for a group of statements describing a particular privacy practice. A statement includes several elements:	
	CONSEQUENCE	An optional, human-readable field that can be used to explain to the user why the specified practice would be valuable in a specific instance.
	PURPOSE	A description of how collected data will be used. Possible values include "current" ("completion and support of the current activity"), "tailoring" ("one-time customization"), "contact" ("contacting visitors for marketing of service or products"), and several others.
	RECIPIENT	The entities that will receive the collected data. Possible values include "ours" ("ourselves and/or entities acting as agents or entities for whom we are acting as an agent"), "delivery" ("delivery services possibly following different practices"), "unrelated" ("unrelated third parties"), and others.
	RETENTION	A description of the policy used to determine when data will be kept by the server. Possibilities include no retention, retention for business practices or legal requirement, and indefinite retention.
	DATA-GROUP and DATA	descriptions of the data that will be collected, possibly falling into a set of categories including physical contact information, financial information, navigation and click stream data, political, health, among others.

Fig. 1. Key elements in the P3P vocabulary [Cranor et al. 2002b].

cookies. As such, they are much less expressive than full policies, and should only be used in conjunction with a complete policy. If the compact policy does not provide enough information for the user agent to act according to the user's preferences, the full privacy policy can be used instead [Cranor et al. 2002a].

User privacy preferences can be described using A P3P Preference Exchange Language (APPEL1.0), defined in a companion specification [Cranor et al. 2002]. APPEL can be used to specify when and with whom a user is willing to exchange data. For example, an APPEL statement (or "ruleset") can be used to specify conditions under which a user might want to block Web sites that engage in certain types of data transfer. An example APPEL rule is given in Figure 3.

As APPEL statements can be fairly complex, users are not necessarily expected to create them directly. The APPEL specification suggests that rulesets would be created by organizations that would distribute them to users. Users could then exchange rulesets with others and copy these rulesets to multiple

```
<POLICIES xmlns="http://www.w3.org/2002/01/P3Pv1">
 <POLICY name="forBrowsers"
     discuri="http://www.catalog.example.com/PrivacyPracticeBrowsing.html"
     xml:lang="en">
 <ENTITY>
   <DATA-GROUP>
    <DATA ref="#business.name">CatalogExample</DATA>
    <DATA ref="#business.contact-info.postal.street">4000 Lincoln Ave.
        </DATA>
    <DATA ref="#business.contact-info.postal.city">Birmingham</DATA>
    <DATA ref="#business.contact-info.postal.stateprov">MI</DATA>
    <DATA ref="#business.contact-info.postal.postalcode">48009</DATA>
    <DATA ref="#business.contact-info.postal.country">USA</DATA>
    <DATA ref="#business.contact-info.online.email">catalog@example.com
        </DATA>
    <DATA ref="#business.contact-info.telecom.telephone.intcode">1
        </DATA>
    <DATA ref="#business.contact-info.telecom.telephone.loccode">248
        </DATA>
    <DATA ref="#business.contact-info.telecom.telephone.number">3926753
        </DATA>
   </DATA-GROUP>
 </ENTITY>
 <ACCESS><nonident/></ACCESS>
 <DISPUTES-GROUP>
  <DISPUTES resolution-type="independent"
    service="http://www.PrivacySeal.example.org"
    short-description="PrivacySeal.example.org">
    <IMG src="http://www.PrivacySeal.example.org/Logo.gif"
         alt="PrivacySeal's logo"/>
    <REMEDIES><correct/></REMEDIES>
   </DISPUTES>
 </DISPUTES-GROUP>
 <STATEMENT>
  <PURPOSE><admin/><develop/></PURPOSE>
  <RECIPIENT><ours/></RECIPIENT>
  <RETENTION><stated-purpose/></RETENTION>
  <DATA-GROUP>
   <DATA ref="#dynamic.clickstream"/>
   <DATA ref="#dynamic.http"/>
  </DATA-GROUP>
 </STATEMENT>
</POLICY></POLICIES>
```

Fig. 2. A simple P3P privacy policy for CatalogExample, a company that collects computer and connection information and page access counts. CatalogExample collects information only for their own purposes, and uses PrivacySeal for dispute resolution [Cranor et al. 2002b].

machines. Rulesets could also be used in collaboration with other tools, such as privacy-sensitive search engines that would only return sites that match user preferences [Cranor et al. 2002].

P3P has undergone significant evolution since its introduction in 1997. Earlier design proposals included additional functionality involving negotiated privacy policies. In this model, if a retrieved privacy policy does not match the user's preference, the user could instruct the browser to return an alternative

```
<appel:RULE behavior="block" description="Service collects personal
                  data for 3rd parties">
     <p3p:POLICY>
         <p3p:STATEMENT>
         <p3p:DATA-GROUP>
           <p3p:DATA>
             <p3p:CATEGORIES appel:connective="or">
               <p3p:physical/>
               <p3p:demographic/>
               <p3p:uniqueid/>
             </p3p:CATEGORIES>
           </p3p:DATA>
         </p3p:DATA-GROUP>
         <p3p:RECIPIENT appel:connective="or">
           <p3p:same/>
           <p3p:other-recipient/>
           <p3p:public/>
           <p3p:delivery/>
           <p3p:unrelated/>
         </p3p:RECIPIENT>
       </p3p:STATEMENT>
     </p3p:POLICY>
</appel:RULE>
```

Fig. 3. An APPEL rule, indicating that the user does not want the site she or he is interacting with to share any physical, demographic, or uniquely identifying information with any other sites [Cranor et al. 2002]. Other possible statements might indicate that a site meeting certain criteria should be accessed, or perhaps that a site should be accessed in a manner that limits the information provided to that site.

policy proposal, or to request an alternative from the Web site. Preliminary proposals also included provisions for managing data transfer between the browser and Web server. User data (name, address, etc.) would be stored in a repository and transferred to the Web site when requested, if the transfer of that data was consistent with user preferences [Reagle and Cranor 1999]. This functionality was removed due to concerns regarding implementation difficulties, lack of interest from Web site operators, and criticisms from privacy activists concerned that this data repository could be a security breach and temptation for unscrupulous operators [LaLiberte 1999].

P3P is only one example of a wide class of tools that provide technical assistance to users desiring greater privacy. Encryption software, anonymous remailers, anonymous/pseudonymous Web browsing proxies, and other tools can be used to provide various forms of privacy in a range of different contexts [Goldberg 2002]. However, as the most visible industry-supported privacy tool, P3P will likely play a particularly influential role.

3. P3P'S PRIVACY MODEL

3.1 Privacy Frameworks

P3P is based upon a model of privacy that has its roots in the five-part privacy model developed by the U.S. Department of Commerce's National Telecommunications and Information Administration (NTIA) and the U.S. Federal

OECD	U.S. FTC	Canadian
Openness	Notice/Awareness	Openness
Purpose Specification		Identifying Purposes
Collection Limitation	Choice/Consent	Consent
		Limiting Collection
Individual Participation	Access/Participation	Individual Access
Data Quality	Integrity/Security	Accuracy
Security Safeguards		Safeguards
Accountability	Enforcement/Redress	Accountability
		Challenging Compliance
Use Limitation		Limiting Use, Disclosure and Retention

Fig. 4. Three proposed models of privacy.

Trade Commission (FTC) [Federal Trade Communication 1996, 1998b; National Telecommunications and Information Administration 1995, 1997]:

(1) *Notice/Awareness*: "Consumers should be given notice of an entity's information practices before any personal information is collected from them" [Federal Trade Commission 1998b]. This information may include identification of the entity collecting the data, the uses of the data, potential recipients, "consequences of a refusal to provide the requested information" [Federal Trade Commission 1998b], and other factors.
(2) *Choice/Consent*: "Giving consumers options as to how any personal data collected from them may be used" [Federal Trade Commission 1998b]. Often described in terms of the "opt-in" vs "opt-out" debate (i.e., whether or not data should be collected without explicit affirmative action by the user), choice may also involve a range of options regarding different purposes.
(3) *Access/Participation*: An individual has the right to view data collected about him or her and to contest the accuracy of that data.
(4) *Integrity/Security*: Data must be accurate and protected against loss or unauthorized access.
(5) *Enforcement/redress*: Effective privacy protection requires some means for ensuring that these principles are applied. Proposed enforcement mechanisms include self-regulation, private remedies, and government action.

The FTC definition of privacy can be compared to alternative, pre-existing definitions such as the models adopted in 1980 by the Organization for Economic Cooperation and Development (OECD) [1980] and in Canada's Personal Information Protection and Electronic Documents Act [Canadian Department of Justice 1998] (Figure 4).

All three definitions contain notions of disclosure, prior consent for information collection and use, individual access to data, and disclosure of details of the collection and use of personal information. However, unlike the FTC model, the OECD and Canadian principles both clearly call for limits on the amount of data collected and the uses of that data. The OECD's "Collection Limitation" principle and the Canadian "Limiting Collection" principles clearly state that there should be limits on the data collected. Both sets of principles require that the purposes that the data will be used for be specified in advance. Any

use of the data for other purposes is prohibited, except with consent of the individual or when required by law. The OECD and Canadian definitions also contain openness principles requiring that "specific information" about policies and practices should be "readily available" [Canadian Department of Justice 1998; Organization for Economic Cooperation and Development 1980].

The FTC definition of notice/awareness is more ambiguous and less straightforward than these disclosures. For example, notice is defined as including "some or all" of a series of criteria, including identification of the data collector, the uses of the data, potential recipients, type of data collected, means of collection, voluntariness of data collection, and data security measures [Federal Trade Commission 1998b]. This relatively vague specification raises the possibility that policies that state who is collecting the data might be interpreted as providing adequate notice, even if they fail to disclose who it might be given to and what it might be used for. Furthermore, the FTC definition does not require that data should be used only for the reasons for which it was collected.

3.2 A Tool for Notice and Choice

P3P's development was clearly aimed at addressing notice and choice: "We believe users' confidence in online transactions will increase when they are presented with meaningful information and choices about Web site privacy practices" [Reagle and Cranor 1999]. The transfer and provision of machine-readable privacy policies can be seen as notice, while user-configurable preferences and the transfer of information based on matches between those preferences and stated policies is a form of choice. P3P defines a standardized, machine-readable format for these policies, along with a protocol for finding them. By making privacy policies easier to find and understand, P3P might help users find the information that they need to make informed decisions regarding the sites they visit. Furthermore, this standard format may provide the basis for the development of automated tools for assessing compliance with privacy laws [Mulligan and Schwartz 2000].

To the developers of P3P, "notice" is defined in terms of objective information aimed at describing existing privacy policies. P3P's design takes great pains to avoid subjective ratings or other judgments. As a result, P3P does not contain any facilities for limiting data flow or determining which sites have acceptable (or unacceptable) privacy policies. Such tools may be built on top of P3P functionality, but they are not part of the specification [Cranor 2002c].

P3P provides limited support for the remaining FTC privacy principles. The "access/participation" principle is handled through the "ACCESS" element (Figure 1). Integrity/security and enforcement/redress are largely concerned with the use and handling of data after it is collected. As such, they are beyond the scope of P3P, which is limited to exchange of information and obtaining consent at the time of data collection.

Although P3P's guiding principles discuss other aspects of privacy, including use limitations, fairness, and integrity [Cranor et al. 2002a], P3P does not address any of these principles directly. Instead, P3P's developers see it as a force that might indirectly lead to implementation of privacy principles such

as use limitation. In this view, the presentation of P3P policies might motivate changes in practice, as companies work to be more consumer friendly. Alternatively, a proliferation of P3P policies that do not meet customer needs might be used as evidence to support arguments for stronger privacy legislation [Cranor and Wenning 2002].

P3P's developers have clearly acknowledged that it is not a complete solution to all of the concerns regarding Internet privacy. In their view, P3P would be one component of a broader strategy for approaching privacy, working alongside regulatory and self-regulatory approaches [Reagle and Cranor 1999] and additional technological tools, perhaps implementing the OECD principles [Cranor and Schwartz 1999].

4. HISTORY

4.1 PICS and Technologies in Support of Self-Regulation

P3P's roots can be found in the Platform for Internet Content Selection (PICS) [Resnick and Miller 1996], a tool for for exchanging information about potentially objectionable content on Web sites. PICS provides a framework for defining rating languages that use numeric scales to describe different types of content. Web site operators or interested third parties can define these languages and use them to rate individual sites. PICS' developers envisioned a wide variety of rating languages that would provide users with a choice of rating schemes that matched their needs and beliefs. As a "values-neutral" protocol that supported the notion of a variety of rating schemes that could be used to tailor descriptions of content to meet certain needs, PICS provides a framework for blocking objectionable content without directly defining exactly which materials would be blocked . The use of PICS to develop "privacy vocabularies" was also suggested [Federal Trade Commission 1996; Resnick and Miller 1996].

PICS was not adopted widely by Web sites, and the range of third-party rating schemes never materialized. However, content-filtering technologies contributed to a major political victory: the defeat of the Communications Decency Act (CDA). The ACLU successfully argued before the Supreme Court that these technologies were "less restrictive" means of preventing children from accessing "indecent" material [ACLU 1996]. In providing a technical solution that helped eliminate the need for a legislative solution, content-filtering tools provided a case study in technical self-regulation of the Internet.

4.2 Political Context

While concerns over pornography and other "adult" material may have been the Internet's first social issue addressed by policymakers, privacy was not far behind. During 1995 and 1996, workshops and reports from the FTC and the NTIA promoted self-regulation as a preferred approach to addressing privacy concerns, along with a "notice and consent" model for privacy protection [Federal Trade Commission 1996; National Telecommunications and Information Administration 1995, 1997; White House 1997]. In 1996, PICS was presented as a technical tool that might be used to address online privacy. The possibility

of multiple PICS-based privacy rating schemes was discussed, along with enhancements, including standard formats that could be used to express user preferences for privacy [Federal Trade Commission 1996].

During 1998–2001, a series of studies on the privacy practices of Web sites was conducted by the FTC [Federal Trade Commission 1998b, 2000], Georgetown University [Culnan 1999], and the Progress and Freedom Foundation [Adkinson et al. 2002]. These studies surveyed both popular and randomly-sampled Web sites for privacy disclosures relating to the FTC privacy principles. Participation in privacy seal programs was also examined [Federal Trade Commission 1999, 2000]. These studies showed increasing prevalence of privacy policies, but the 2000 report expressed concern over the slow pace of improvement. This concern led the FTC to recommend privacy legislation that would "set forth a basic level of privacy protection for all visitors to consumer-oriented commercial web sites" [Federal Trade Commission 2000]. In 2001, new FTC Chair Timothy J. Muris took a more cautious stand on privacy legislation, calling instead for increased enforcement of existing laws [Muris 2001].

Several legislative measures aimed at protecting Internet privacy were introduced during the 105th and 106th Congresses [Center for Democracy and Technology 2001a, 2001b]. Of these, the Children's Online Privacy Protection Act (COPPA), which placed restrictions on collection of information from children, was the only legislation enacted [Center for Democracy and Technology 1998]. Meanwhile, at various government hearings, P3P advocates described the possibilities for P3P as part of a self-regulatory regime [Schwartz 2001; Scoblionkov 1998], perhaps as a complement to legislation [Mulligan 1998].

Privacy advocates, who had never been satisfied with the emphasis on self-regulation [Federal Trade Commission 1996], continued to push for legislation [Clausing 1999], establishment of a federal privacy agency, enforcement of fair information practices, development of techniques to limit the collection of information [Rotenberg 1999], and other more stringent measures.

4.3 Technical Efforts

The use of PICS as a technical tool for protecting privacy was suggested at FTC privacy workshops in November 1995 [Federal Trade Commission 1998b] and June 1996 [Federal Trade Commission 1996]. In the fall of 1996, the Internet Privacy Working Group (IPWG) was organized by the Center for Democracy and Technology, with the goal of developing technical specifications to provide a framework for supporting fair information practices. IPWG developed a draft privacy policy and worked with W3C to develop a prototype tool. This work led to the start of the W3C's P3 (the original name for P3P) project [Cranor 2002c], which formally started in May 1997, with a projected 18-month time frame for the development of a tool for privacy protection [Miller 1997]. Figure 5 provides a brief overview of the P3P's history.

Development work continued through 1998–2000. Concerns over a patent claim that may have covered P3P proved distracting, until a W3C legal analysis concluded that the patent in question was not relevant [Rein et al. 1999;

October 1995	NTIA White Paper: "Privacy and the NII: Safeguarding Telecommunications-Based Personal Information" introduces notice & choice model of privacy in a self-regulatory context [National Telecommunications and Information Administration 1995a].
June 1996	FTC Workshop on Consumer Privacy in the Global Information Infrastructure discusses possibility of extending PICS to protect personal data [Federal Trade Commission 1996].
November 1996	The Center for Democracy and Technology forms the Internet Privacy Working Group (IPWG) to work on a privacy tool based on PICS [Cranor 2002c].
June 1997	NTIA report on "Privacy and Self-Regulation in the Information Age" [National Telecommunications and Information Administration 1997b].
July 1, 1997	Clinton administration's "Framework for Global Electronic Commerce" advocates self-regulation as preferred approach to privacy protection [White House 1997].
July 10, 1997	P3P Kickoff meeting at W3C. Initial participants include AT&T, Microsoft, and the Direct Marketing Association. Project expected to last 18 months [Miller 1997].
October 30, 1997	W3C announces completion of P3P stage 1 [World Wide Web Consortium 1997]. Development work continues through 1998-2000
May 19, 1998	W3C publishes first public draft of P3P 1.0 specification [World Wide Web Consortium 1998].
Summer 1998	W3C alerted as to possible conflict with Intermind patent [World Wide Web Consortium 2002b].
July 21, 1998	At FTC hearing on privacy in cyberspace, the Direct Marketing Association mentions P3P as an example of self-regulation [Scoblionkov 1998].
May 3, 1999	W3C announces a public effort to gather information for fighting the Intermind patent [Sullivan 1999].
September 21, 1999	W3C issues note describing removal of data transfer facilities from P3P [LaLiberte 1999].
October 28, 1999	W3C patent analysis confirms P3P does not infringe upon Intermind patent [Rein et al. 1999].
June 22, 2000	W3C holds P3P Interop in New York City, with around 100 participants. Several user agents and P3P policy editors were demonstrated, along with more than a dozen P3P-compliant web sites [Weitzner 2000].
March 22, 2001	Microsoft introduces Internet Explorer 6.0, with support for the use of P3P to handle preferences for web browser cookies [Microsoft 2001a].
January 28, 2002	W3C issues proposed recommendation for P3P 1.0 [Cranor et al. 2002b].
April 16, 2002	W3C issues P3P 1.0 as a Recommendation [World Wide Web Consortium 2002c].

Fig. 5. An abbreviated history of P3P's development.

World Wide Web Consortium 2002b]. Initial development of P3P seemed to near completion in 2000, as a P3P interoperability event held in June demonstrated several prototypes of P3P-compliant software [Weitzner 2000]. However, feedback from the event resulted in additional specification revisions that took several more months to complete and required another round of public vetting. On March 22, 2001, Microsoft announced Internet Explorer 6.0, which includes P3P functionality for restricting Web site cookies [Microsoft 2001a; Walker 2001]. AT&T's Privacy Bird, an Internet Explorer plug-in supporting P3P functionality, was released in the spring of 2002 [AT&T 2002]. On April

16, 2002, almost five years after the initial P3P kickoff, the W3C released the P3P1.0 specification as a recommendation [Cranor et al. 2002b].

4.4 User Agent Software: P3P in Web Browsers

User agent software that manages user interactions during Web browsing is a critical component of P3P. This software is used to specify privacy preferences and to respond to conflicts between user preferences and site policies. When faced with these conflicts, user agents may take one or more of a number of actions, including blocking access to sites, providing dialog boxes warning of potential privacy risks, displaying passive feedback, or blocking cookies.

P3P's developers have implemented a series of interface prototypes, which have been refined through a series of user tests [Cranor 2002c]. AT&T's "Privacy Bird" [AT&T 2002] is an add-on for Internet Explorer that can process and interpret P3P policies. Privacy Bird provides a dialog box containing 12 checkboxes that can be used to select a variety of privacy practices, along with radio buttons to choose "low," "medium," or "high" privacy, based on preconfigured selections from those 12 options. APPEL policies can also be imported.

The Privacy Bird takes the form of an icon that is placed directly in the Internet Explorer title bar. When the user visits a Web site, the bird's color is adjusted to reflect the privacy implications of the site for the user: a green bird indicates a site that is safe to visit; a yellow bird indicates that the site is not P3P-enabled; and a red bird indicates a conflict between site policies and user preferences. As a tool that handles complete privacy policies, Privacy Bird provides a demonstration of many of P3P's possibilities.

Microsoft's Internet Explorer 6.0, which was released in 2001, is the first mass-market Web browser to provide integrated support for P3P. IE 6.0 uses a "privacy thermostat" to support a 5-point scale ranging from "low" to "high" privacy, with increasingly stricter restrictions on the Web site cookies that will be accepted. The "privacy thermostat" is implemented using the familiar interface metaphor of a slider, similar to a volume control, that can be dragged to the desired setting. IE 6.0's cookie management facilities are based only on compact P3P policies. Netscape Navigator, IE 6.0's main competitor, does not support P3P in its 6.0 release, but preview versions of Netscape 7 have P3P functionality comparable to that of IE 6.0.

5. TECHNICAL CRITIQUES

5.1 Scope and Limitations

P3P addresses a relatively narrow conception of privacy, limited to the principles of notice and choice [Reagle and Cranor 1999] regarding the privacy implications of interactions with Web sites. The collection and use of personal information is tacitly assumed: P3P does not provide any mechanisms for imposing limits on the collection and use of data, as proposed in other models of privacy [Canadian Department of Justice 1998; Organization for Economic Cooperation and Development 1980]. Instead, use limitation is assumed to occur indirectly, as the transparency provided by P3P convinces vendors to adopt

privacy policies that meet consumer needs [Cranor and Wenning 2002]. Furthermore, privacy of e-mail and other online activities is beyond the scope of P3P, which is limited to Web interactions.

P3P's developers have repeatedly discussed their concerns regarding the proposal's limitations and implications. Perhaps the most immediate and important disclaimer regards the lack of enforcement mechanisms. P3P was intended to support notice and choice, but it was never intended to police the operators or enforce adherence to stated privacy policies. Although P3P "does not provide a technical mechanism for making sure sites act according to their policies," it is "complementary to laws and self-regulatory programs that can provide enforcement mechanisms" [Cranor et al. 2002b]. Specifically, existing laws prohibiting deceptive practices, such as the FTC Act [Federal Trade Commission 1998a], can be used to enforce Web site privacy promises in the U.S. Inclusion of enforcement mechanisms would have been extremely difficult, requiring access to databases and data exchange practices by information collectors. Unfortunately, the lack of enforcement mechanisms might not be clear to users, who may base their decisions upon incorrect assumptions regarding the enforcement of P3P functionality.

The P3P team has acknowledged the difficulty of managing complex privacy policies and preference statements. P3P's privacy policy vocabulary supports a wide range of statements for describing data that will be collected and the uses that will be made of that date. Similarly, APPEL can be used to specify complicated preferences for information disclosure according to the uses to which it will be put and the practices of the collecting organization. Although this flexibility may be necessary for supporting a wide range of practices and user preferences, it presents significant challenges for users who may be overwhelmed by too many choices.

The use of predefined APPEL rulesets might address this problem of specifying preferences, but it remains to be seen whether or not this multiplicity of choices will materialize. Past experience with PICS does not provide much encouragement: despite a design that encouraged multiple alternative ratings schemes, only a handful of PICS schemes were widely used.

5.2 Vocabulary

The vocabulary used to describe data transfer practices (and user preferences) is a critical component of P3P. As the basis for P3P policy files, the vocabulary defines what can (and cannot) be said in a P3P policy. Although the terms in the P3P vocabulary are not intended to be presented directly to users, they may form the basis for terminology used in user agent software. This terminology may in turn be used to present information about privacy policies or solicit user preferences. As a result, any ambiguities in P3P's vocabulary can directly impact a user's understanding of site privacy policies.

Perceived shortcomings of P3P's vocabulary (Figure 1) have been a target of substantial criticism. For example, the RECIPIENT field includes values such as "ours," which indicates "ourselves and/or entities acting as our agents or entities for whom we are acting as an agent" [Cranor et al. 2002b]. This definition

describes the sharing of information from the viewpoint of the Web site operator, who is presumably well-informed about the group of entities that might fall under this umbrella. However, the breadth of this description might create some difficulties for users. If P3P interfaces display this definition in its entirety, users are likely to be confused by the definition of an "agent," and users who want to avoid sharing information with any third party may wonder why more restrictive options are not available. Alternatively, simplified definitions aimed at helping users might (perhaps intentionally) omit necessary distinctions, perhaps leading users to conclude that data would not be shared with any entities. Additional values for the recipient field might help the development of policies that would meet the expectations of many users. For example, a value stating "this site only" might be used to indicate that data collected on a site would only be used within the context of specific Web site.

Similarly, "PURPOSE" contains values such as "current," indicating the "completion and support of activity for which data was provided" [Cranor et al. 2002b], without defining the scope of that activity. Under this definition, the "current activity" might be interpreted as purchasing a book or as establishing a commercial relationship, leading to significantly different privacy implications. P3P currently does not contain a vocabulary for more precise definitions of these primary uses of data. The other values of "PURPOSE," including "develop," "tailoring," "telemarketing," "historical," and others, are uses that go beyond the immediate purpose for which the data was collected. Thus, P3P can be used to indicate that shopping cart information from a Web store will be used for customizing the content displayed on a site ("tailoring"), but it cannot be used to provide any specific details about how information will be used to complete the current transaction. More specific values such as "payment," "delivery," and "Web search" have been proposed to eliminate some of this ambiguity [Thibadeau 2000].

The "ACCESS" element illustrates some of the tensions involved in developing privacy vocabularies. This element indicates "whether the site provides access to various kinds of information," but "the method of access is not specified" [Cranor et al. 2002b]. As P3P was explicitly designed to describe data practices without commenting on their appropriateness, the definition of the "ACCESS" element includes the value "none," which could be used to indicate that access to identifying data is not provided. Even though a lack of access provisions would appear to contradict the spirit of the FTC's "Access/participation" principle, the "none" value is necessary to support Web sites that wanted to use P3P without changing their data practices. The inclusion of "access" was in itself controversial, as some commentators felt that it inappropriately defines the principle of data access as an important component of privacy [Cranor 2002c]. The "ACCESS" element and the principle upon which it is based [Federal Trade Commission 1998b] present a host of challenges in terms of implementation details and policies that are beyond the scope of the P3P specification [Cranor 2002c].

Earlier versions of the data model were criticized as being asymmetric, with data describing users far outweighing data about the operators of the Web sites [Coyle 1999]. This criticism appears to have been at least partially addressed by

the "ENTITY" element, which requires the inclusion of the entity's name and contact information in P3P-compliant privacy policies [Cranor et al. 2002b]. P3P's vocabulary does contain "DISPUTES" and "REMEDIES" elements that provide information about how the vendor might resolve problems or complaints, but these options are not required and are only useful for addressing privacy violations, not preventing them.

Despite the inclusion of terms such as "ENTITY," "DISPUTES," and "REMEDIES," the vocabulary is still relatively limited in terms of information that might be used by consumers to assist in their informed use of privacy policies. Appropriate additions to the vocabulary might provide users with more relevant information. As mentioned above, the addition of a recipient value "this site only" might help privacy-conscious Web users identify those situations where their data might be used only on a single site. Similarly, the "ENTITY" field might be augmented with "agents" information, which might provide pointers to other entities that data might be shared with, thus clarifying the "ours" value for the "RECIPIENT" field.

The process of converting nuanced practices and attitudes towards privacy into a computer-readable vocabulary may be inherently problematic. The "formalization of human constructs" has been identified as a possible source of bias in computer systems: the very process of converting subtle distinctions into rigid categories may introduce bias [Friedman and Nissenbaum 1997]. More colloquially, "formal systems are too rigid to encompass real life" [Oram 2000].

As P3P's vocabulary has not been tested against user perceptions and expectations, the extent of this potential bias may not be known. General end-user attitudes towards privacy have informed the P3P process [Cranor et al. 1999], but end-users were not involved in the development of the vocabulary. Although testing with a representative sample of Internet users is clearly impossible, empirical trials with end-users might have helped identify possible sources of confusion between user perceptions and P3P definitions.

5.3 User Agents

Designers of P3P user agents face the daunting challenge of providing accurate information about privacy practices in a manner that helps users understand the impact of their choices regarding different information practices. If end-user tools are confusing or hard to use, P3P's impact will be minimized. This has been a concern throughout the course of the P3P project. P3P developers described the design of interfaces for supporting P3P as "inherently complex, ill-defined, and seemingly unsolvable" [Ackerman and Cranor 1999]. Privacy critics—intelligent agents that would provide suggestions and warnings to users—were proposed as a possible solution [Ackerman and Cranor 1999]. Approaches that simplify the vocabulary and language used might reduce the complexity of the user interface, but these simplifications may confuse users and lead them to draw false conclusions [Cranor 2002c].

Past experience with browser-based cookie control functions in Netscape and Internet Explorer demonstrate the potential pitfalls. Both Netscape and Internet Explorer were found to have interface design problems that hindered

comprehension of cookie practices and limited effective disclosure of relevant information. For example, cookie control facilities were often located three menu levels deep in the user interface, making them difficult to find [Millett et al. 2001]. IE 6.0's P3P interface may present problems in this regard, as three menu selections must be made to access the P3P control panel. Moving the privacy settings to a separate menu, or perhaps as a button on the toolbar, might improve usability [Millett et al. 2001].

Effective use of IE 6.0's privacy thermostat might also be hindered by language that obscures the exact meaning of the various levels of privacy protection. Potentially confusing language in the original IE 6.0 announcement describing cookies as "unsatisfactory" [Microsoft 2001a] was replaced with distinctions between first- and third-party cookies [Microsoft 2001b], but these differences may not be obvious to many users. The privacy thermostat uses other terminology that may be difficult to comprehend, including phrases such as "compact privacy policy," ambiguous distinctions between "blocking" and "restricting" cookies, and other undefined terms such as "implicit consent" and "personally identifiable information." Given this use of potentially confusing terminology, IE 6.0's implementation of P3P may not be sufficiently comprehensible to meet some definitions of informed consent [Millett et al. 2001].

As many users can be expected to leave default settings unchanged, IE 6.0's defaults also raise concerns. The "privacy thermostat" comes preconfigured with a "medium" level of privacy protection. This might provide some amount of protection, but it is not at all clear that this "adoption by default" can be seen as providing meaningful privacy protection that meets user expectations.

IE 6.0 handles only "compact" P3P policies [Cranor et al. 2002b] and not the longer, more detailed, policies. This limits the privacy thermostat to addressing the use of cookies. Collection of personal information is not discussed, thus exempting sites that collect and exchange personal information without using cookies from the P3P model. This focus might create an installed base of Web sites and users who view P3P as a cookie management tool, ignoring the other privacy concerns that might be addressed by a more complete implementation of P3P.

AT&T's Privacy Bird addresses many of the shortcomings of IE 6.0's privacy thermostat. As an icon that resides directly on the title bar, the Privacy Bird avoids the potential usability problems associated with controls located deep in an applications menu structure. Terminology and visual representations used in Privacy Bird have been revised based on feedback gathered during a series of user tests [Cranor 2002c]. The Privacy Bird also goes beyond IE 6.0 to handle complete policies, thus supporting the use of P3P to describe a wider variety of data practices.

The main weakness of the Privacy Bird software lies in its implementation as a browser plug-in that must be downloaded and installed by users. The effort required to use Privacy Bird might discourage users and limit its impact. The primary contribution of Privacy Bird and other add-on tools may be as design suggestions that would influence future versions of integrated P3P tools in Internet Explorer and other browsers.

If designed appropriately, P3P user agent software might help manage or reduce P3P's complexity, but the prospects for such solutions may depend on the complexity of privacy practices and preferences. Pessimistic views of the difficulty of appropriate interface design are based in the perception of privacy as involving a set of numerous variables, each of which must be assessed separately for each relationship between a Web user and a Web site [Ackerman and Cranor 1999]. In the face of this complexity, designers might be faced with the choice of either building complicated interfaces or introducing simplifications that may obscure important details, and therefore increase the difficulty of making an informed choice. However, if privacy preferences and practices are not very complex, interface design might be a less daunting task.

6. POLICY CRITIQUES

6.1 The Notice and Choice Privacy Model

Many advocates take a view of privacy that is different from the notice and choice model underlying P3P. To these critics, privacy is a right, to be protected by fair information practices such as those found in the OECD or Canadian principles [Catlett 1999; Electronic Privacy Information Center 2000; Hunter 2000]. In place of the notice and choice model, these advocates argue for standards that would limit the collection and dissemination of personal data. For advocates in the U.S., this might mean new legislation [Catlett 1999; Oram 2000] in a manner that is consistent with existing U.S. law regarding privacy implications of other technologies [Electronic Privacy Information Center 2000]. To the extent that P3P discusses preferences in the context of ongoing data exchange, without limiting the data that is actually exchanged, P3P is seen as a tool that fails to address privacy [Coyle 1999]. Furthermore, the reliance on choice is seen as being inconsistent with established norms that discourage models that commoditize privacy [Electronic Privacy Information Center 2000].

Specific aspects of P3P's implementation of the notice and choice model have also been criticized. The complexity associated with a vocabulary that can be used to describe a wide range of privacy preferences has been described as being unnecessary for describing user preferences: "the core of consumers' desires for privacy are simple and easily stated, but unpalatable for marketers: consumers don't want their personal information sold, shared, or reused for secondary purposes" [Catlett 1999]. While this claim about user preferences might be difficult to validate, it is possible that an alternative vocabulary that focused on user preference (instead of vendor practices) might have been simpler.

Critics have also raised concern over the legitimacy of the notice that is provided by P3P. In addition to language and complexity issues that might make P3P statements hard to interpret [Coyle 1999; Oram 2000; Thibadeau 2000], changes in the uses of data and in privacy statements have been identified as concerns. Specifically, the continual evolution of data mining techniques and other analysis tools might make it impossible for data collectors to adequately describe future uses of data that is collected. Changes in products, services,

business practices, and business relationships might also lead to changes in data practices. Mindful of these possible changes, some sites reserve the right to amend their privacy policies at any time. The possibility that a company's data usage and privacy statement might change over time is seen as limiting the utility of any notice that may be provided [Hunter 2000].

The claim that P3P will lead to the implementation of practices that protect privacy has also come under fire. Concerns have been raised that vendors will not provide policies that provide meaningful privacy protection, and practices will not change as a result of consumer preferences [Catlett 1999]. In some cases, consumers may not have the option of avoiding sites with unappealing data practices in favor of alternatives: if sites provide unique content, or if alternative sites do not provide better policies, users may be faced with the choice between privacy and services. In other cases, sites that use data exchange to support lower prices for goods may simply leave users with the implicit choice of having to pay to protect their privacy [Coyle 2000].

Other, less desirable, potential outcomes of P3P have also been identified. For example, Web site operators concerned about the potential drawbacks of providing users with too much information about data practices [Lee and Speyer 1998] might stop supporting P3P if disclosure leads visitors to stay away from their sites [Hunter 2000].

These criticisms apply mainly in the U.S. Non-U.S. Internet users in domains with strong Internet privacy laws may find that P3P provides a useful adjunct to legal requirements that implement privacy codes that limit data collection.

Most of the discussion about the impact of P3P—both pro and con—remains hypothetical. Evaluation of practical outcomes will require critical masses of P3P-enabled Web sites, widely available P3P-compliant browsers, and users who are both educated and motivated to use P3P. This delay is unappealing to privacy advocates who argue that Internet users should not have the protection of their privacy subjected to large-scale experiments with unknown results [Catlett 1999].

Hypothetical claims about potential outcomes of P3P raise the question of assessment. In particular, how will the impact of P3P be evaluated? Rigorous evaluation of P3P's use might present the best assessment of its impact, but it is not at all clear how this evaluation might be conducted. Such an assessment would require definitions of meaningful metrics for success, possibly including (but not limited to), the rate of P3P compliance among major commercial Web sites, rate of use of nondefault privacy settings, and user perceptions of privacy and P3P's role. Some of these measurements would be technically difficult to collect, as they would require collecting data directly from user agent software—data that might itself raise privacy concerns.

Alternatively, P3P might be evaluated by assessing its impact on privacy practices. Using an approach similar to the FTC Web surveys of privacy practices [Federal Trade Commission 1998b, 2000], popular Web sites might be sampled to determine the impact of P3P on their privacy practices. If the introduction of P3P was shown to have some correlation with changes that moved privacy policies closer to fair information practices, this might be seen as a success. Similarly, patterns in complaints to regulators such as the FTC

or third-party privacy seal organizations might be examined in order to see if P3P had any impact.

6.2 P3P and Self-Regulation

Some privacy activists have rejected the notion of self-regulation, arguing that it will not provide meaningful privacy protection, as industry's goal is to avoid legislative or regulatory constraints on business practices [Catlett 1999; Rotenberg 2001]. This claim has been aimed at the development of P3P. Specifically, P3P is described as an effort in (somewhat) bad-faith technological development—a "Pretext for Privacy Procrastination"—with the goal of presenting an appearance of protecting privacy [Catlett 1999]. In this viewpoint, the completion of technical work and the deployment of systems built on the protocol are unimportant, so long as laws are not passed and legislation is not enacted. This interpretation has been the subject of a public dialog [Catlett 1999; Cranor and Schwartz 1999].

This controversy raises some questions regarding the evaluation of technological proposals in the context of this self-regulation regime. P3P was never the sole component of self-regulatory efforts, as privacy policies and privacy seal programs such as TRUSTe [TRUSTe 2002] play crucial roles. However, to the extent that P3P plays a role in self-regulation, its success or failure can be seen as a factor in evaluating the success of privacy self-regulation as a whole.

Consideration of P3P's role in self-regulation requires an examination of the "self" that is involved. P3P's organizational home, the World Wide Web Consortium, is a group of industrial, academic, and nonprofit organizations that works to define technical specifications for Web infrastructure [World Wide Web Consortium 2002a]. Industrial participants in the W3C working group on P3P included AT&T, Microsoft, IBM, the Direct Marketing Association, and others [DesAutels 1997]. The P3P group also included nonprofit privacy advocates from the Center for Democracy and Technology (CDT), who played a vocal role in supporting P3P [Mulligan 1998; Mulligan and Schwartz 2000]. Representatives of data protection authorities from France, Canada, Germany, and Hong Kong also participated [Cranor 2002b]. Several other prominent privacy advocates did not participate in the P3P process, and have been vocal critics of P3P [Catlett 1999; Coyle 1999; Electronic Privacy Information Center 2000].

To the extent that the industrial participants were and do take part in activities that involve Internet privacy issues, P3P seems to be an example of a self-regulatory effort. However, many Internet companies such as Amazon.com were not involved, despite the privacy-sensitive nature of their businesses. Presumably, the developers of P3P hope that these companies will participate by providing P3P-compliant policies once the technology is deployed, but the companies' absence raises questions about the eventual prospects for P3P. Some businesses may "opt-out" of P3P for fear that the protocol would provide too much information about their information practices [Lee and Speyer 1998]. Alternatively, other organizations might be concerned that P3P does not provide enough granularity to describe information practices in a manner that is consistent with existing natural language policies [Allen 2001].

The pace of development efforts—more than four years from project announcement to the release of any significant P3P-compliant user agent software—has been cited as supporting the interpretation of P3P as a tool for delaying or avoiding regulatory action [Catlett 1999]. P3P supporters responded to these criticisms by arguing that the "deliberative and thoughtful process" behind P3P led to the delays, and that the inclusiveness of the P3P project was the main reason for the delays [Cranor and Schwartz 1999]. W3C archives of P3P draft specifications provide evidence of ongoing work: numerous revisions of the draft specification have been published. Changes made during this time included additions that addressed some of the issues raised in criticisms of earlier drafts, such as the need for vocabulary elements covering topics such as remedies and disputes [Cranor 2002b].

The delays in the development and deployment of P3P are not necessarily surprising or indicative of any intentional stalling. The process of creating a technical standard for a controversial topic such as privacy is almost guaranteed to be slow and laborious. Distractions, such as the controversy over a patent that may have covered parts of P3P, may also have contributed to delays. The perceived complexity of privacy policies [Cranor and Reagle 1998] and user interfaces [Ackerman and Cranor 1999] required for P3P deployment may have complicated matters further. The time scale of P3P's development is comparable to that of at least one related effort, the Internet Engineering Task Force's five-year process of developing standard for Web-browser cookies [Kristol 2001].

However legitimate and understandable these delays may have been, they may also have served a useful political purpose for proponents of self-regulation. If development work had stopped completely, or had never been started, the self-regulatory model might have been subject to more aggressive scrutiny, perhaps leading to legislation or regulation. Completion of P3P had costs as well, as a finished specification might have led (and might still lead) to pressures for adoption and deployment—technical efforts that might require significant resources. A protracted development process allowed industry to enjoy the benefits of P3P without paying the costs: proponents could point to the existence of P3P as proof that a self-regulatory process was working, without having to face any of the expenses and risks associated with deployment of a completed specification.

P3P critics have also pointed to industry portrayals of P3P as evidence of the protocol's role as a political tool. Although the developers of P3P have always been careful to note that P3P was not a complete solution to Internet privacy concerns [Cranor et al. 2002b; Reagle and Cranor 1999] others have not always been so cautious. Industry groups like the Direct Marketing Association (DMA) have been accused of over-selling the benefits and availability of P3P [Catlett 1999]. P3P's developers objected to the portrayal of P3P as an attempt to derail the political process, arguing that "nothing in the P3P specification or the P3P guiding principles presumes that P3P is designed to replace public policy or a public policy process" [Cranor and Schwartz 1999].

These contrasting views of P3P's role in privacy self-regulation are not necessarily inconsistent. It should not be surprising that P3P's virtues would be

excessively praised by those who saw it as a potentially powerful political tool, despite the cautions expressed by the development team. The portrayal of P3P as a bad-faith effort aimed only at avoiding legislation seems less plausible than that of a legitimate, if somewhat frustrating, attempt to meet the goal of building a technology to address a highly politicized social concern.

The role of P3P in bolstering the self-regulatory model is hard to assess. FTC reports in 1998 and 1999 expressed a clear reluctance to interfere with industry on the basis of lack of progress in providing privacy policies [Federal Trade Commission 1998b, 1999]. These reports did not look to P3P to support their argument for self-regulation, but the promise of a technological cure-all that promised imminent solutions to a thorny problem may have played a role in convincing government regulators that action was unnecessary. The FTC changed its position in 2000, citing insufficient progress as justification for recommending privacy legislation [Federal Trade Commission 2000]. It is conceivable that an earlier deployment of P3P might have provided enough progress to render this recommendation unnecessary.

P3P might play a role in influencing the content of future legislative or regulatory proposals. P3P has garnered support among members of Congress: a Congressional resolution introduced in 2001 expressed the sense of the House that P3P was an important tool for Internet privacy [Smith 2001]. Future proposals for privacy legislation might include incentives and legal protections for sites that use P3P, possibly together with the establishment of additional responsibilities for Web site operators. For example, legislation might require the use of P3P for certain sites, reduce or eliminate liability for privacy violations for sites that use P3P, or provide penalties for sites that use P3P to defraud or mislead users. If these laws supported the use of P3P without placing further requirements upon Web site operators, they would effectively provide legal support for P3P's self-regulatory model.

6.3 P3P, PICS, and the Role of Third Parties

In the PICS model, third parties were seen as providers of ratings services, supplying descriptions of content to suit a range of values [Resnick and Miller 1996]. The P3P specifications propose a different role for third parties, as providers of APPEL "rulesets" that could be used to describe a user's privacy preferences [Cranor and Reagle 1998; Cranor et al. 2002].

An alternative model might involve third parties as privacy rating organizations. In this model, consumer groups might offer ratings of the privacy practices of various online entities, and user agent software could be configured to retrieve ratings from these third parties before visiting Web sites. These ratings could go beyond the information provided in P3P policy statements, perhaps informing users of customer complaints or regulatory actions regarding each site. The possibility of third party privacy ratings was suggested as an extension of PICS, before the P3P project started [Federal Trade Commission 1996]. Current PICS tools could theoretically be used alongside P3P to provide this functionality, possibly using the P3P vocabulary as the basis for ratings [Cranor 2002c].

Alternatively, P3P might be extended to provide limited opportunity for inclusion of external information. For example, APPEL profiles might be extended to include a "BLACKLIST" field. This field would contain a third party URL that would list known privacy violators [Cranor 2002a]. Given this field in an APPEL preference statement, the user's browser could periodically retrieve the blacklist and warn the user when any of the sites on that list are visited. Although such a tool would require appropriate changes to the specifications, it is certainly technically feasible, and the effort required to build a blacklist of a few tens or hundreds of Web sites would be significantly less than the work required to build a generalized third party privacy rating system.

Extending P3P to allow third party comments or blacklists would amount to a fundamental change in the balance of power and information control in P3P. The current specification leaves vendors and Web site operators as the sole commentators on their practices. Extensions that allow external groups or individuals to discuss a site's information practices would remove this control over the discourse, creating a situation where vendors might find their practices painted in an unfavorable light.

Some Web site operators might see P3P as a tool that limits their control over privacy policies. Before the advent of P3P, the content and formatting of privacy policies were completely under the control of the site operator. To be P3P-compliant, sites must augment these free-form policies with P3P policies containing specific information using terms defined in P3P's vocabulary. Some industry representatives have noted that this creates the possibility that P3P statements might not contain details found in plain-text privacy policies [Allen 2001]. The P3P development team has acknowledged the possible difficulties by modifying the specification to indicate that P3P policies should use terms that match practices as closely as possible, without making any misleading statements [Weitzner and Cranor 2002].

Influencing the balance of power over discussion of privacy may not have been a conscious goal behind design decisions. In particular, it is certainly possible that this level of vendor control arose as a byproduct of architectural decisions made for other reasons. The question of intent—"was P3P designed to give Web site operators control over discussion of privacy?"—may be less important than the practical reality that P3P's design might be perceived as having this result. For critics who have seen P3P as taking a view of privacy as defined by Web site operators, a larger role for third parties might make P3P more appealing.

The design of the P3P may have additional unintended consequences that allow the tool to be used in ways not discussed in the specifications. For example, third parties might build tools that automatically retrieve and interpret privacy policies. These tools could be used to construct and maintain centralized archives suitable for privacy comparisons between competitive vendors. If P3P is widely adopted, other novel uses of P3P data may arise after users and businesses gain practical experience with P3P-compliant tools.

6.4 P3P as Defining Privacy

If P3P is widely used, its definition of privacy might be seen or promoted as the final word in defining online privacy. This concern has been raised by those who worry that P3P's narrow approach will promote an inadequate conception of privacy: the European Union's working party on the protection of individuals with regards to the processing of personal data expressed concerns that P3P "has instead sought to formalize lower common standards" [European Commission Working Party on the Protection of Individuals with regard to the Processing of Personal Data 1998].

The deployment of P3P features in IE 6.0 may be a factor in institutionalizing a particular view of privacy and P3P. Microsoft's position in the marketplace almost guarantees widespread adoption of IE 6.0, and, therefore, of Microsoft's interpretation of P3P. If Web site operators dedicate significant resources in creating privacy policies that are compatible with IE 6.0's use of P3P, they might be reluctant to dedicate further resources toward creating complete policies. IE 6.0's market share makes this "lock-in" a real possibility, and creates a significant disincentive for any others who might suggest an alternative user model for P3P. IE 6.0's reliance on compact policies raises the possibility that sites might provide compact policies without full policies. This would allow them to avoid having cookies blocked by IE 6.0, without having to incur the costs of becoming fully P3P-compliant. Furthermore, IE 6.0's focus on cookies might create an installed base of Web sites and users who view P3P as a cookie management tool, ignoring the other privacy concerns that might be addressed by a more complete implementation of P3P.

P3P might also influence perceptions of the role that technologies can play in protecting privacy. In particular, P3P might be presented as the technological limit of what can be done to protect privacy. Descriptions of the complexity of P3P essentially take this view, describing some difficulties in the building of the system as essentially unsolvable [Ackerman and Cranor 1999]. These appropriate and honest academic discussions of challenging design problems can easily be extended to bolster claims that more effective privacy controls are simply technically impossible: "We do not know how to build systems that are any more complex than P3P, . . . so P3P is the best technology for privacy that we will be able to provide." This argument would deflect discussion of the problem from the underlying business and policy choices that create the complexity to a discussion of the limits of technology.

Portrayals of P3P as the limit of what can be achieved through technical measures do not originate with P3P's developers, who have consistently pointed out P3P's limits and their associated design challenges [Ackerman and Cranor 1999; Cranor and Reagle 1998; Reagle and Cranor 1999]. In fact, members of the P3P development team have expressed support for technologies that implement all of the OECD privacy principles [Cranor and Schwartz 1999]. This openness about the limits of the technologies might not prevent others from cynically portraying P3P as some sort of definitive technological approach to privacy.

6.5 P3P as a Public Process

P3P was (and is) very much part of a political process. As an example of a self-regulatory tool, P3P is a policy proposal in the form of a technical mechanism: in Lessig's terms, a choice of architecture over law as an effective regulator [Lessig 1999]. As such, it should be discussed and analyzed just as any legal or regulatory proposal.

Since the beginning of the P3P process, the development team has invited public participation in the form of comments on specifications [Mulligan and Schwartz 2000], and has repeatedly warned about the limits of P3P [Reagle and Cranor 1999; Mulligan and Schwartz 2000]. The P3P team has responded publicly to numerous criticisms and suggestions regarding the protocol, leading to public exchanges between P3P's developers and its critics [Catlett 1999; Cranor and Schwartz 1999].

However, this support for public participation has an important limitation. P3P's basis on the notice and choice model for privacy was assumed from the start of the project. This assumption was implicit: the P3P development team did not write or distribute a requirements document [Cranor 2002b]. Public comments on the P3P proposal were solicited and received after the initial goals and scope of the project were determined, but this input was not used to reconsider the definition of privacy underlying P3P.

The choice of the notice and choice privacy model was a fundamental design decision that determined the scope of the project and led to the debates over P3P's legitimacy as a privacy protection tool. For privacy advocates who argue for limits on the collection and exchange of sensitive data about individual consumers or citizens, the notice and choice model is inadequate. Faced with a proposal based on this definition of privacy, some privacy advocates were bound to reject P3P, and were unlikely to participate in any public discussions that did not consider the possibility of broader views of privacy.

These debates over the legitimacy of P3P might have been addressed through open and inclusive discussion of the goals and specifications for a technological system to protect the privacy of Internet users. Such a process might have eliminated controversy, developed trust among the various parties, and possibly even paved the way for quicker adoption.

This deliberation might have been accomplished through public meetings, online discussions, or publications of requirements documents or social impact statements [Shneiderman and Rose 1997] describing the tradeoffs—as far as they were understood—associated with privacy and the design of any technical proposal. Ideally, participants on all sides of the debate would have access to the statements and viewpoints that led to any decision regarding the content of any technical proposal, and the process that led to a consensus (or lack thereof) would have been clearer.

There is no guarantee that this deliberative process would have led to a workable solution. This discussion might have led to proposals that were broader in scope and definition than P3P, perhaps going beyond notice and choice to address other privacy goals. These broader proposals might have failed to generate any consensus regarding scope and definition of privacy protection tools.

Without such consensus, widespread acceptance of an effective tool would have been unlikely, and the project might have failed.

This view of social protocols as public policy proposals might not be accepted by organizations that sponsor development of technical protocols. P3P's organizational home, the W3C, disclaims any responsibility for setting policy: "The W3C is merely a standard setting organization; it does not have the ability to determine public policy" [Cranor and Schwartz 1999], and "W3C does not wish to become the forum for public policy debates" [Mulligan and Schwartz 2000]. Although these statements may be technically true, they fail to account for the significant influence of the W3C and the pivotal role that the P3P vocabulary may play in privacy debates. As a consortium that includes many large software vendors, Internet companies, and the developers of the Web browsers used by the vast majority of Web users [World Wide Web Consortium 2002d], the W3C develops protocols that shape how data is manipulated, exchanged, and accessed over the World Wide Web. To the extent that the Web is seen as a tool for discourse, education, access to government information and services, these standards are in some sense determining the policies for a public medium.

Designers of P3P user agents also have a role to play in the success or failure of P3P as a public process. While the development of the P3P specification was conducted in a somewhat public manner, P3P user interfaces were developed by software vendors following relatively closed practices. Tools such as AT&T's Privacy Bird may have been informed by repeated user testing, but these designs were not subject to the comments and revisions that have been ongoing throughout the development of the specification. Vendors of user agent software are therefore in a powerful (and unaccountable) position regarding the future of P3P.

Given the critical nature of user agent software, expanding the specification to include discussion of requirements for user interfaces might have been appropriate. However, the wide range of behaviors and tools that might be used for P3P present a significant challenge in developing a specification that provides sufficient detail without overwhelming or over-constraining developers. Alternatively, the P3P developers might have provided fully-developed example interfaces for discussion during the public comment process.

7. P3P AND SOCIAL PROTOCOLS

As the Internet continues to evolve, a growing number of situations with proposed technical solutions to social concerns may arise. Anonymity (or its prevention), online reading, copyright protection, unsolicited email (spam), and computer crime are just some of the current concerns that involved both technology and policy. Tools built to address these issues provide mechanisms for achieving policy goals, but perhaps also encourage or allow a variety of possibly unintended consequences.

To successfully navigate the complexities of the interplay between technology and policy, both technologists and policy-makers must take a somewhat wider view of their crafts, with technologists incorporating policy analysis into their

designs, and policy-makers carefully examining the implications of technical decisions. In the case of P3P, more thorough cross-disciplinary analysis may have identified some concerns that still remain unresolved. For the technicians, examination of the contexts of deployments and the assumptions underlying the design proposal might have revealed some of the overly optimistic elements of P3P. Similarly, a careful analysis of the contents of the P3P specification might have led regulators to reconsider its viability as a technology for self-regulation.

P3P's history illustrates the difficulty of creating and deploying these technical solutions. Although originally proposed in 1997, P3P was not widely available to consumers until Microsoft's Internet Explorer 6.0 was released in 2001. Users who have installed IE 6.0 and configured the privacy thermostat may find them to be of limited use until P3P-compatible privacy policies become commonplace.

The debates and discussion over the development of P3P provide a variety of lessons for future social protocols:

—*Technological solutions to social problems are likely to be defined by nontechnical, contextual issues*: The definition of P3P as a system for supporting notice and choice was based on an implicit assumption behind the P3P project. Similarly, future social protocols may have their basis in social and political discussions that predate technical efforts. As these discussions may shape the scope and capabilities of the resulting technologies, awareness of their impact and examination of underlying assumptions may be necessary.

—*Technology can mask the political nature of the debates over social protocols*: Many of the discussions about the perceived strengths and weaknesses of P3P were really debates over proper and appropriate definitions of privacy. Discussions about the specific details of technical proposals may have the effect of limiting debate to include only those who have appropriate technical training and resources.

—*Technology may raise unrealistic expectations*: Both PICS and P3P have been seen at various times as complete solutions, even when developers have cautiously discussed their limitations. The lure of the "silver bullet" may lead to similarly inflated expectations of social protocols. Particularly with controversial topics such as privacy, the temptation to assume that a technological fix can wipe away political difficulties may prove too strong to resist.

—*Technical processes may be used for political ends*: Despite cautious disclaimers of P3P's limits and calls for legislation from some P3P supporters, others used P3P as a tool to promote self-regulation and argue against privacy legislation. Given the politically charged nature of privacy, this is not surprising. To be most effective, developers of future social protocols might need to complement their technical knowledge with the political savvy necessary to avoid or minimize any "co-opting" of their efforts.

—*Formal definitions may not be sufficient for describing complex social activities*: The critiques of the P3P vocabulary illustrate the difficulty of defining a small set of terms that adequately and clearly defines a wide range of practices. This may lead to intentional and unintentional bias [Friedman and

Nissenbaum 1997], confusion, and lack of clarity that may prevent the tools from being used as intended.

—*Social protocol designs should include user interface considerations when appropriate*: Despite the acknowledged difficulty of building user interfaces for P3P [Ackerman and Cranor 1999], the P3P specifications say relatively little about interface design. The inclusion of proposed user interfaces in specification drafts provided for public comment might have prompted commentary and evaluation. This feedback might have helped both in the design of improved interfaces and in identifying elements of the vocabulary and protocol that might have proven difficult for end-users to understand.

—*End-user tools and social protocols require end-user participation*: As P3P's vocabulary was not tested against the perceptions of nontechnical Internet users, there is a the very real possibility that end-user confusion might render the privacy notices incomprehensible and subsequent decisions meaningless. "Field-testing" of the definitions and assumptions behind social protocols may be necessary.

—*Assessment is important*: The debates over P3P have included a range of claims and counter-claims about possible outcomes of P3P when widely deployed. For developers to learn from the successes or failures of P3P or similar protocols, assumptions and theories that guide design should be tested when possible.

8. CONCLUSION

The controversy in recent discussions of Internet privacy creates substantial challenges for any proposal aimed at addressing the problem. The development of P3P was at least partially motivated by the hope that a technical solution would be able to provide effective privacy protection while avoiding the difficulties faced by legislative and regulatory proposals. However, the decision to approach privacy from a technical viewpoint did not eliminate any of the difficulties surrounding data collection, use, and retention. As a result, the P3P developers were faced with the difficult task of combining the essentially political task of creating a working definition of some aspects of privacy with the technical task of defining the protocol details.

The extent of P3P's impact remains to be seen, but the process of its development bears striking similarities to legislative and regulatory proposals. Strong differences of opinion between interested parties led to numerous revisions and extensions to definitions, goals, and terminology; participants in the process were accused of acting in bad faith; P3P was used as a rhetorical tool to support political agendas; and the process took far longer than planned.

Developers of future social protocols may face similar problems. Early acknowledgment of the potentially political nature of these technical proposals, along with public discussions of their scope and definition, might help avoid some of the difficulties faced by the developers of P3P. As controversy and debate may be unavoidable, these discussions should ideally address the overall applicability of technical approaches. When complexities and political disputes make social protocols ineffective, the most effective approach might be to forego

the use of technological approaches and move discussion into social and political contexts.

APPENDIX–GLOSSARY

APPEL A P3P Preference Exchange Language: a computer-readable framework for expressing user privacy preferences (http://www.w3.org/TR/P3P-preferences.html). APPEL profiles are compared to P3P privacy policies to determine whether or not a given Web site poses privacy concerns for the user.

IE Microsoft's Internet Explorer Web browser.

FTC The U.S. Federal Trade Commission (http://www.ftc.gov).

NTIA The U.S. National Telecommunications and Information Administration (http://www.ntia.doc.gov).

OECD The Organization for Economic Cooperation and Development (http://www.oecd.org).

P3P The Platform for Privacy Preferences (http://www.w3.org/p3p).

PICS The Platform for Internet Content Selection, a protocol for rating Internet content, and a precursor of P3P (http://www.w3.org/pics).

W3C The World Wide Web Consortium (http://www.w3.org).

XML The Extensible Markup Language—the data transfer language used to express P3P privacy policies and APPEL privacy preference profiles (http://www.w3.org/xml).

ACKNOWLEDGMENTS

Thanks to Mark Ackerman, Jason Catlett, Jean Camp, Karen Coyle, Patrick Feng, Brian Kahin, Andy Oram, Marc Rotenberg, Barbara Simons, Ben Shneiderman, Judith Yanowitz, and the anonymous reviewers for their helpful comments. Special thanks to Lorrie Cranor for her assistance.

REFERENCES

ACKERMAN, M. AND CRANOR, L. 1999. Privacy critics: UI components to safeguard users' privacy. In *Proceedings of ACM Conference on Human Factors in Computing Systems, Extended Abstracts*. ACM Press, New York, 258–259.

ACLU. 1996. Reno v. ACLU supreme court brief.

ADKINSON, W., EISENACH, J., AND LENARD, T. 2002. Privacy online: A report on the information practices and policies of commercial web sites. http://www.pff.org/publications/privacyonlinefinalael.pdf.

ALLEN, C. 2001. Bits financial service roundtable, comments on P3P (1.0) specification working draft of 24 Sept. 2001. http://lists.w3.org/Archives/Public/www-p3p-public-comments/2001Oct/att-0015/01-BITS_comments.DOC.

AT&T. 2002. At&T privacy bird. http://www.privacybird.com.

CANADIAN DEPARTMENT OF JUSTICE. 1998. Privacy provisions highlights. http://canada.justice.gc.ca/en/news/nr/1998/attback2.html.

CATLETT, J. 1999. http://www.junkbusters.com/standards.html.

CENTER FOR DEMOCRACY AND TECHNOLOGY. 1998. Children's online privacy protection act of 1998 (COPPA). http://www.cdt.org/legislation/105th/privacy/coppa.html.

CENTER FOR DEMOCRACY AND TECHNOLOGY. 2001a. 105th Congress: Legislation affecting the internet. http://www.cdt.org/legislation/105th/privacy/.

CENTER FOR DEMOCRACY AND TECHNOLOGY. 2001b. 106th Congress: Legislation affecting the internet. http://www.cdt.org/legislation/106th/privacy/.

CLAUSING, J. 1999. FTC asked to examine data profiling services. *New York Times*, Nov. 9. http://www.nytimes.com/library/tech/99/11/cyber/capital/09capital.html.

COYLE, K. 1999. P3P: Pretty poor privacy? a social analysis of the platform for privacy preferences (P3P). http://www.kcoyle.net/p3p.html.

COYLE, K. 2000. A response to "P3P and privacy: An update for the privacy community" by the Center for Democracy and Technology. http://www.kcoyle.net/response.html.

CRANOR, L. 2002a. Personal communication.

CRANOR, L. 2002b. The role of privacy advocates and data protection authorities in the design and deployment of the platform for privacy preferences. In *Proceedings of Computers, Freedom, and Privacy, 2002*. ACM Press, New York, 1–8. http://doi.acm.org/10.1145/543482.543506.

CRANOR, L. 2002c. *Web Privacy with P3P*. O'Reilly and Associates, Sebastopol, CA.

CRANOR, L., LANGHEINRICH, M., MARCHIORI, M., PRESLER-MARSHALL, M., AND REAGLE, J. 2002a. The platform for privacy preferences 1.0 (P3P1.0) specification. W3C recommendation 28 Jan. 2002. http://www.w3.org/TR/2002/PR-P3P-20020128/.

CRANOR, L., LANGHEINRICH, M., MARCHIORI, M., PRESLER-MARSHALL, M., AND REAGLE, J. 2002b. The platform for privacy preferences 1.0 (P3P1.0) specification. W3C proposed recommendation 16 April 2002. http://www.w3.org/TR/P3P/.

CRANOR, L., MARCHIORI, M., AND LANGHEINRICH, M. 2002. A P3P preference exchange language 1.0. W3C working draft 15 April 2002. http://www.w3.org/TR/P3P-preferences/.

CRANOR, L. AND REAGLE, J. 1998. Designing a social protocol: Lessons learned from the platform for privacy preferences. In *Telephony, the Internet, and the Media*, J. Mack-Mason and D. Waterman, Eds. Lawrence Erlbaum Associates, Mahwah, NJ.

CRANOR, L., REAGLE, J., AND ACKERMAN, M. 1999. Beyond concern: Understanding net users' attitudes about online privacy. Tech. Rep. TR 99.4.3, AT&T Labs-Research. http://www.research.att.com/resources/trs/TRs/99/99.4/99.4.3/report.htm.

CRANOR, L. AND SCHWARTZ, A. 1999. Response to Catlett's "open letter to P3P developers". http://www.w3.org/P3P/catlett-letter.txt.

CRANOR, L. AND WENNING, R. 2002. Why P3P is a good privacy tool for consumers and companies. http://www.gigalaw.com/articles/2002-all/cranor-2002-04-all.html.

CULNAN, M. 1999. Georgetown internet privacy policy survey: Report to the Federal Trade Commission. http://www.msb.edu/faculty/culnanm/GIPPS/gipps1.pdf.

DESAUTELS, P. 1997. Platform for privacy preferences (p3) project. http://www.w3.org/P3P/100797Update.html.

MULLIGAN, D. AND SCHWARTZ, A. 2000. P3P and privacy: An update for the privacy community. http://www.cdt.org/privacy/pet/p3pprivacy.shtml.

ELECTRONIC PRIVACY INFORMATION CENTER. 2000. Pretty poor privacy: An assessment of P3P and internet privacy. http://www.epic.org/Reports/prettypoorprivacy.html.

EUROPEAN COMMISSION WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA. 1998. Platform for privacy preferences (P3P) and the open profiling standard (ops): Opinion of the working party. http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp11en.htm.

FEDERAL TRADE COMMISSION. 1996. Public workshop on consumer privacy on the global information infrastructure. http://www.ftc.gov/reports/privacy/privacy1.htm.

FEDERAL TRADE COMMISSION. 1998a. FTC fact sheet, Jan. 30, 1998: Relevant statutes enforced by the Federal Trade Commission. http://www.ftc.gov/opa/1998/9801/factshet.htm.

FEDERAL TRADE COMMISSION. 1998b. Privacy online: A report to Congress. http://www.ftc.gov/reports/privacy3/toc.htm.

FEDERAL TRADE COMMISSION. 1999. Self-regulation and privacy online: A Federal Trade Commission report to Congress. http://www.ftc.gov/os/1999/9907/privacy99.pdf.

FEDERAL TRADE COMMISSION. 2000. Privacy online: Fair information practices in the electronic marketplace: A Federal Trade Commission report to Congress. http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

FRIEDMAN, B. AND NISSENBAUM, H. 1997. Bias in computer systems. In *Human Values and the Design of Computer Technology*, B. Friedman, Ed. CSLI Publications, Stanford, CA, 21–40.

GOLDBERG, I. 2002. Privacy-enhancing technologies for the internet II: Five years later. In *PET 2002 Workshop on Privacy-Enhancing Technologies*. Lectuers Notes in Computer Science. Springer-Verlag, Berlin.

HUNTER, C. 2000. Recoding the architecture of cyberspace privacy: Why self-regulation and technology are not enough. http://www.asc.upenn.edu/usr/chunter/net_privacy_architecture.html.

KRISTOL, D. 2001. HTTP cookies: Standards, privacy, and politics. *ACM Trans. Internet Technol. 1*, 2 (Nov.), 151–198.

LALIBERTE, D. 1999. Removing data transfer from P3P. http://www.w3.org/P3P/data-transfer.html.

LEE, K. AND SPEYER, G. 1998. White paper: Platform for privacy preferences project (P3P) and citibank. http://www.w3.org/P3P/Lee_Speyer.html.

LESSIG, L. 1999. *Code and Other Laws of Cyberspace*. Basic Books, New York.

MICROSOFT. 2001a. Microsoft P3P implementation in internet explorer 6.0 and windows fact sheet. http://www.microsoft.com/PressPass/press/2001/Mar01/PrivacyToolsIEfs.asp.

MICROSOFT. 2001b. Use security and privacy features in Internet Explorer 6. http://www.microsoft.com/windowsxp/pro/using/howto/security/ie6.asp.

MILLER, J. 1997. The platform for privacy preferences (p3) project. http://www.w3.org/P3P/P3_overview_JM.html.

MILLETT, L., FRIEDMAN, B., AND FELTEN, E. 2001. Cookies and web browser design: Toward realizing informed consent online. In *Proceedings of ACM Conference on Human Factors in Computing Systems (CHI 2001)*. ACM Press, New York, 46–52.

MULLIGAN, D. 1998. Testimony before the senate committee on commerce, science, and transportation subcommittee on communications, Sept. 23, 1998. http://www.cdt.org/testimony/980923mulligan.shtml.

MURIS, T. J. 2001. Protecting consumers' privacy: 2002 and beyond remarks of FTC chairman Timothy J. Muris. http://www.ftc.gov/speeches/muris/privisp1002.htm.

NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION. 1995. Privacy and the NII: Safeguarding telecommunications-related personal information. http://www.ntia.doc.gov/ntiahome/privwhitepaper.html.

NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION. 1997. Privacy and self-regulation in the information age. http://www.ntia.doc.gov/reports/privacy/privacy_rpt.htm.

ORAM, A. 2000. Promises, promises, promises. http://www.cpsr.org/cpsr/nii/cyber-rights/web/p3p_promises.html.

ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT. 1980. Recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data. http://europa.eu.int/comm/internal_market/en/dataprot/inter/priv.htm.

REAGLE, J. AND CRANOR, L. 1999. The platform for privacy preferences. *Commun. ACM 42,* 2 (Feb.), 48–55.

REIN, B., STEPHENS, G., AND LEBOWITZ, H. 1999. Analysis of P3P and u.s. patent 5,862,325. http://www.w3.org/TR/P3P-analysis.html.

RESNICK, P. AND MILLER, J. 1996. Pics: Internet access controls without censorship. *Commun. ACM 39,* 10 (Oct.), 87–93.

ROTENBERG, M. 1999. EPIC testimony on Internet privacy before the Subcommittee on Courts and Intellectual Property, Committee of the Judiciary U.S. House of Representatives. May 27, 1999. http://www.epic.org/privacy/internet/EPIC_testimony_599.html.

ROTENBERG, M. 2001. Fair information practices and the architecture of privacy (what Larry doesn't get). *Stanford Technology Law Rev*.

SCHWARTZ, A. 2001. Utilizing privacy controls in data transfer technologies. Statement before the Federal Trade Commission Workshop on "The information marketplace: Merging and exchanging consumer data". March 13, 2001. http://www.cdt.org/testimony/010313schwartz.shtml.

SCOBLIONKOV, D. 1998. E-commerce gets one last chance. *Wired News*, July 21. http://www.wired.com/ news/politics/0,1283,13895,00.html.

SHNEIDERMAN, B. AND ROSE, A. 1997. Social impact statements: Engaging public participation in information technology design. In *Human Values and the Design of Computer Technology*, B. Friedman, Ed. CSLI Publications, Stanford, CA, 117–133.

SMITH, A. 2001. Adam Smith leads P3P privacy resolution. http://www.house.gov/apps/list/press/wa09_smith/010607pr.html.

SULLIVAN, J. 1999. Volunteer army to fight patent. *Wired News*, May 3. http://www.wired.com/news/ politics/0,1283,19452,00.html.

THIBADEAU, R. 2000. A critique of P3P: Privacy on the web. http://dollar.ecom.cmu.edu/p3pcritique.

TRUSTE. 2002. Truste: Make privacy your choice. http://www.truste.com.

WALKER, L. 2001. Browser aimed at protecting users' privacy. *Washington Post*, March 29.

WEITZNER, D. 2000. June 21 2000 platform for privacy preferences (P3P) project interop report. http://www.w3.org/P3P/p3p-interop-report-20000621.html.

WEITZNER, D. AND CRANOR, L. 2002. Response to bits (19 June 2002) letter re: Legal status of P3P policy statements. http://lists.w3.org/Archives/Public/www-p3p-public-comments/2002Jul/0001.html.

WHITE HOUSE. 1997. A framework for global electronic commerce. http://eleccomm/ecomm.htm.

WORLD WIDE WEB CONSORTIUM. 1997. World Wide Web Consortium announces completion of P3P project phase one: Industry leaders collaborate to ensure user privacy concerns are respected on the Web (October 30, 1997). http://www.w3.org/P3P/press_release.html.

WORLD WIDE WEB CONSORTIUM. 1998. W3C publishes first public working draft of P3P1.0: Collaborative efforts by key industry players and privacy experts promote Web privacy and commerce (May 19, 1998). http://www.w3.org/Press/1998/P3P.html.

WORLD WIDE WEB CONSORTIUM. 2002a. About the World Wide Web Consortium (W3C). http://www.w3.org/Consortium/.

WORLD WIDE WEB CONSORTIUM. 2002b. P3P and privacy faq. http://www.w3.org/P3P/P3Pfaq.html.

WORLD WIDE WEB CONSORTIUM. 2002c. World Wide Web Consortium issues P3P 1.0 as a W3C recommendation. http://www.w3.org/2002/04/p3p-pressrelease.

WORLD WIDE WEB CONSORTIUM. 2002d. World Wide Web Consortium (W3C) members. http://www.w3.org/Consortium/Member/List.

Received April 2002; accepted August 2002