User Interfaces for Privacy Agents

LORRIE FAITH CRANOR[1] [2]
Carnegie Mellon University

PRAVEEN GUDURU
AT&T Labs

MANJULA ARJULA
AT&T Labs

Most people do not often read privacy policies because they tend to be long and difficult to understand. The Platform for Privacy Preferences (P3P) addresses this problem by providing a standard machine-readable format for web site privacy policies. P3P user agents can fetch P3P privacy policies automatically, compare them with a user's privacy preferences, and alert and advise the user. Developing user interfaces for P3P user agents is challenging for several reasons: privacy policies are complex, user privacy preferences are often complex and nuanced, users tend to have little experience articulating their privacy preferences, users are generally unfamiliar with much of the terminology used by privacy experts, users often do not understand the privacy-related consequences of their behavior, and users have differing expectations about the type and extent of privacy policy information they would like to see. We developed a P3P user agent called the AT&T Privacy Bird. Our design was informed by privacy surveys and our previous experience with prototype P3P user agents. We describe our design approach, compare it with the approach used in other P3P use agents, evaluate our design, and make recommendations to designers of other privacy agents.

Categories and Subject Descriptors: H.5.2 [Information Interfaces and Presentation]: User Interfaces—evaluation/methodology
General Terms: Human Factors
Additional Key Words and Phrases: P3P, privacy, user agent, preferences, privacy policy, privacy enhancing technology

---

1. INTRODUCTION

As individuals spend more time online, they are becoming increasingly concerned about Internet privacy. Most individuals have little knowledge about the real risks to their privacy in an online environment and they find learning about privacy and reading web site privacy policies to be difficult and time consuming [41]. Software tools have been developed to assist users in protecting their privacy online. Often referred to as Privacy Enhancing Technologies (PETs), these tools include software for hiding a user's online identity, encrypting communications, and managing HTTP cookies [5,9,10,23]. Many of these PETs have been made available as research prototypes or free open source software. Their developers have typically focused on the underlying cryptographic

[1] School of Computer Science, 5000 Forbes Ave, Pittsburgh, PA 15213 <lorrie@acm.org>

algorithms or other technical aspects of the software, without devoting much attention to usability [47]. As a result, most of these tools have failed to gain widespread adoption outside communities of technical experts. As new PETs are being developed that are intended for use by the general public, research is needed to determine how to develop user interfaces that will be most accessible and allow individuals to take best advantage of the underlying technical tools to protect their privacy.

With the release of the Platform for Privacy Preferences (P3P) specification in 2002 [13], we are seeing the emergence of a new type of PET designed to provide users with information about web site privacy policies. In some cases these P3P privacy "agents" can not only inform users, but also take actions automatically on the basis of this information, for example blocking cookies at web sites that have privacy policies that don't meet some minimum threshold for privacy protection.

In Section 1 we introduce the P3P specification and discuss its role in privacy protection. In Section 2 we discuss challenges faced by designers of privacy agents. In Section 3 we describe how we addressed these challenges as we developed a P3P user agent called the AT&T Privacy Bird. In Section 4 we compare our approach with the approach taken by designers of other P3P user agents. In Section 5 we present the results of a user survey and a laboratory study in which we evaluated Privacy Bird and compared it with another P3P user agent. Finally, in Section 6 we conclude with a discussion of our results, the social implications of privacy agents, and recommendations for future work.

The Platform for Privacy Preferences

Privacy policies are notoriously time consuming to read and difficult to understand [27,41,42]. The World Wide Web Consortium (W3C) addressed this problem by developing P3P, a standard computer-readable language for web site privacy policies. The P3P 1.0 Specification provides an XML syntax in which web sites can express their privacy policies as well as standard mechanisms for web browsers and other software to locate and fetch these policies [10,13]. P3P user agents can be built into web browsers, browser add-ons, proxies, or other software. These user agents may check for P3P policies at web sites a user visits, compare them with users' previously specified privacy preferences, and provide feedback to the user about these policies. Thus users need not read privacy policies at every site they visit. Some user agents make cookie-blocking decisions on the basis of P3P policies or take other actions such as allowing or denying

[2] This work was performed while the author was employed by AT&T Labs-Research.

access to a user's electronic wallet. In the future, P3P-enabled search engines may allow users to include privacy preferences among their search criteria [7].

The P3P 1.0 Specification [13] defines a P3P "vocabulary" that includes eight major components, most of which contain multiple sub-components and attributes. Each component is represented as an XML element. For example, data usage is represented by the "purpose" element. The specification defines 11 purpose sub-elements, each representing a data use. In addition, each of these purpose sub-elements has a "required" attribute that indicates whether the data may be used for this purpose all the time, on an opt-in basis, or on an opt-out basis. Figure 1 gives an overview of the major P3P policy components. The purpose, data, recipients, retention and consequence elements are bundled together into a structure called a P3P "statement." A P3P policy contains one or more statements. Sites use the statement structure to indicate types of data that are treated in similar ways. For example, a site might have one statement to describe the information it stores in log files, and one statement to describe the information it collects from individuals who make purchases at the site. Figure 2 shows an example of a P3P policy for a web site that collects only the data stored in standard server log files.

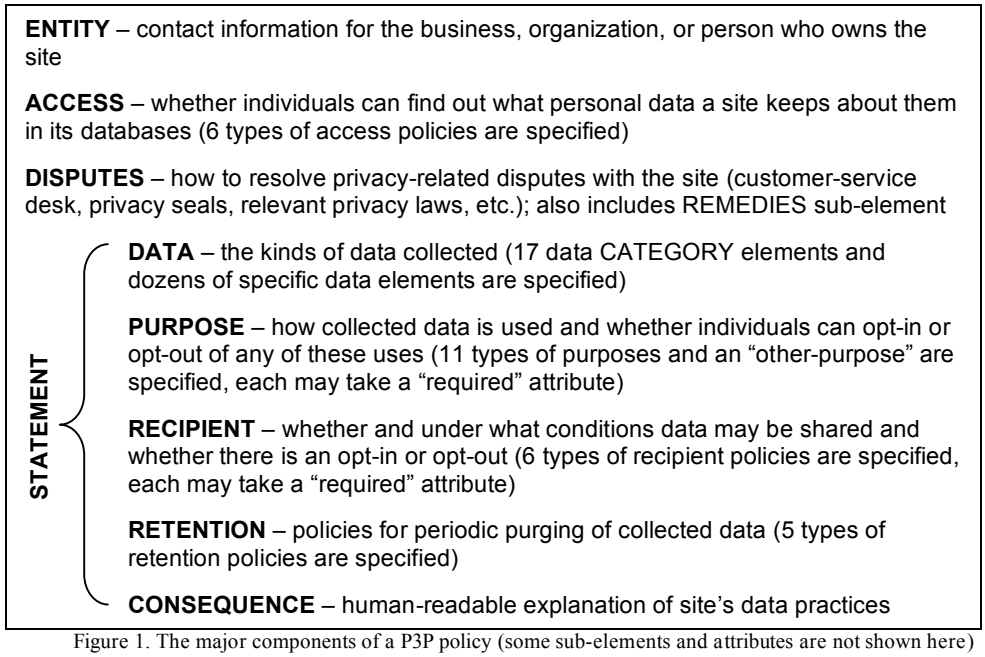

Figure 1. The major components of a P3P policy (some sub-elements and attributes are not shown here)

```
<POLICIES xmlns="http://www.w3.org/2002/01/P3Pv1">
<POLICY discuri=http://p3pbook.com/privacy.html name="policy">
  <ENTITY>
    <DATA-GROUP>
      <DATA
```

```
        ref="#business.contact-info.online.email">
        privacy@p3pbook.com
      </DATA>
      <DATA
        ref="#business.contact-info.online.uri">
        http://p3pbook.com/
      </DATA>
      <DATA ref="#business.name">Web Privacy With P3P</DATA>
    </DATA-GROUP>
  </ENTITY>
  <ACCESS><nonident/></ACCESS>
  <STATEMENT>
    <CONSEQUENCE>Our Web server collects access logs containing
      this information.
    </CONSEQUENCE>
    <PURPOSE><admin/><current/><develop/></PURPOSE>
    <RECIPIENT><ours/></RECIPIENT>
    <RETENTION><indefinitely/></RETENTION>
    <DATA-GROUP>
      <DATA ref="#dynamic.clickstream"/>
      <DATA ref="#dynamic.http"/>
    </DATA-GROUP>
  </STATEMENT>
</POLICY>
</POLICIES>
```

Figure 2. A P3P policy for a web site that collects only the data stored in standard server log files. This policy contains a single STATEMENT element, which indicates that the data is collected to complete the current transaction, for website and system administration, and for research and development; that the data is used only by the website and its agents; and that the data may be retained indefinitely.

The P3P 1.0 Specification also includes syntax for a P3P "compact policy," an abbreviated version of an XML P3P policy that describes a web site's data practices with respect to cookies. Compact policies consist of combinations of three-letter tokens, many of which can be modified by a compact version of the required attribute to indicate whether opt-in or opt-out opportunities are provided. Fifty-two such tokens are specified. P3P compact policies are optional for P3P-enabled web sites; they are used to facilitate rapid cookie-blocking decisions. However, because compact policies do not include a token similar to the STATEMENT element, they tend to over simplify a site's privacy practices, making them appear more invasive than they actually are. For example, a web site that explains in its full P3P policy that it collects preference information that it may share with other companies and physical contact information that it will not share, would create a compact policy that states that it collects both preference information and physical contact information and that it may share both types of information. New compact policy syntax has been proposed for P3P 1.1 that would allow web sites to make clearer compact policy statements [46].

A separate W3C specification called A P3P Preference Exchange Language (APPEL)[3] specifies an XML encoding for user preferences about privacy policies [14]. APPEL is a rule-based language. P3P user agents can compare APPEL rules with a P3P policy to determine whether or not a site's policy matches a user's preferences. Writing APPEL rule files is fairly difficult, even for experts, and thus it is not expected that end users will create APPEL rule files themselves. Users may export APPEL rule files produced by one P3P user agent and import them into another. In addition, organizations with privacy expertise might make APPEL rule files available on their web sites.

P3P policies were designed both to provide information about website privacy policies that a human might use to make decisions (such as whether or not to shop at a particular web site or whether to exercise "opt-out" options), and to facilitate automated decision-making (such as whether to display a privacy warning or whether to block cookies at a particular web site). The details of how a P3P user agent might use a P3P policy to display information[4] or to make automated decisions are not part of the P3P 1.0 Specification; instead they have been left to user agent implementers. Implementers thus face questions about how much information to present, what words to use, what aspects of privacy policies to emphasize, and how to make this information most accessible to end users. They also face questions about how to elicit privacy preferences from users, the range of configuration options to offer, and the types of decisions that should be automated. These questions can be grouped into two major interface design challenges: an interface for informing users about web site privacy policies, and an interface for configuring a P3P user agent to take actions on the basis of a user's privacy preferences.

The Role of Privacy Enhancing Technologies

Most discussions of PETs begin by referencing a set of principles known as Fair Information Practices (FIPs). Several formulations of FIPs have been developed since the 1970s. The Organization for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data are, perhaps, the most well known. Codified in 1980, the OECD Guidelines include the following eight principles [38]:

---

[3] APPEL is considered somewhat experimental and is not supported by all P3P user agents. Unlike P3P 1.0, APPEL is a *W3C Note,* not an official *W3C Recommendation*. Recommendation status is reserved for specifications that have gone through W3C's extensive review process, have been voted on by the W3C membership, and have been approved by the W3C director. APPEL has not gone through this process.

[4] The P3P 1.1 specification is expected to include guidelines for displaying P3P policy information in plain language for end users. Many of the guidelines in the draft P3P 1.1 specification are based on the language used in our Privacy Bird interface.

Collection Limitation Principle: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the Purpose Specification Principle except: a) with the consent of the data subject; or b) by the authority of law.

Security Safeguards Principle: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

Openness Principle: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle: An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability Principle: A data controller should be accountable for complying with measures which give effect to the principles stated above.

Many privacy laws, industry privacy guidelines, and self-regulatory privacy programs are based on some or all of these principles. PETs can be described in terms of which of these principles they support. For example, encryption tools may support the security safeguards principle and anonymity tools may support the collection limitation principle. P3P primarily supports the purpose specification and openness principles, which are sometimes referred to collectively as "notice." P3P does not support the other FIPs directly. A P3P user agent might include encryption and anonymity tools, thus expanding its scope with respect to the FIPs. In addition, through increased transparency about data practices, P3P user agents might indirectly support other FIPs. For example, when P3P user agents make clear to the public the extent to which a company shares data, that company might decide to change its practices and limit data disclosure. However, there is no guarantee that P3P deployment will result in such policy changes.

In jurisdictions without comprehensive privacy laws, PETs can play an important role in allowing individuals to proactively protect their own privacy. However, users of PETs often have to trade off convenience and functionality for privacy protection. For example, web anonymity tools typically slow web browsing and prevent users from using web site features that rely on javascript. To be effective, some PETs require cooperation from other parties. For example, anonymous electronic cash systems may be useful only if an individual frequents a vendor who accepts anonymous electronic cash payments. The usefulness of P3P user agents is limited by P3P adoption. As more web sites adopt P3P, P3P user agents will allow users to quickly understand privacy policies at these sites. If P3P is widely adopted, users may be able to use P3P user agents to identify sites with the best privacy policies. In addition, the transparency of privacy policies brought about by P3P may motivate sites to improve their privacy practices.

In jurisdictions where laws are in place that reflect most or all of the FIPs, the role of PETs may not be immediately obvious. However, in these jurisdictions PETs also play an important role as privacy laws do not ban all potentially privacy-invasive practices. Indeed, the FIPs suggest that individuals should be offered choices and the ability to control the use of their data. Reading privacy notices and making choices can be time consuming, and tools that automate a user's ability to control the flow and use of their personal information can minimize the effort necessary to exercise control. Furthermore, use of these tools helps ensure that users will retain some control even when their web surfing takes them to jurisdictions without comprehensive privacy laws [37].

2. DESIGN CHALLENGES

Designing a user interface for specifying privacy preferences is challenging for several reasons: privacy policies are complex, user privacy preferences are often complex and nuanced, users tend to have little experience articulating their privacy preferences, users are generally unfamiliar with much of the terminology used by privacy experts, and users often do not understand the privacy-related consequences of their behavior. Designing a user interface for informing users about privacy policies is challenging for many of the same reasons. In addition, this task is complicated by the fact that users have differing expectations about the type and extent of privacy policy information they would like to see. Thus user interface designers need to find ways to manage the complexity, educate users about privacy or express privacy concepts using language they already understand, guide users through the process of expressing their privacy preferences, and offer various options that meet the needs of a diverse set of users.

Complex Privacy Policies

As already discussed, P3P privacy policies include eight major components, most of which include sub-components. Some components are represented as elements for which there are fixed sets of possible values, while others are represented by elements that can include text strings or extensible sets of possible values. User privacy preferences often reflect a combination of privacy policy components. For example, a user may wish to receive a warning at sites that collect financial information and use it for marketing, but not at sites that collect financial information and use it to provide financial services, nor at sites that collect preference information and use it for marketing. Even if we limit our discussion to those elements with fixed sets of possible values and ignore the attributes that may modify these elements, there are over 36,000 possible combinations of privacy policy components that can be expressed using the P3P syntax. Potentially, users may wish to express a preference over any of these combinations. When attributes and human-readable elements are brought into the discussion, the problem is further complicated.

In some ways our task is simplified by the fact that we are developing tools that rely on policies encoded using a limited syntax; however, the fact that this syntax may not fully capture all privacy policy information that may be of interest to users may serve to complicate matters. When designing a P3P user agent that people will find useful, we must hope that the P3P syntax is able to convey enough of the complex details of privacy policies to allow the tool to provide the functions users desire. If desired functions require access to privacy policy information that cannot be encoded in a P3P policy, then we will be unable to provide them without developing mechanisms outside the scope of P3P, if at all. Because our iterative design and testing process significantly overlapped the P3P specification development process, feedback from our test subjects did have an impact on the design process. Nonetheless, some information desired by users was ultimately not included in P3P, or included only as an optional field. For example, while some of our test subjects expressed an interest in seeing a complete list of the companies their information might be shared with, most companies are unwilling to include such information in their privacy policies or in a P3P policy. Thus the technical, political, resource, and other constraints that limited the expressiveness of the P3P vocabulary may also limit the capabilities of P3P user agents.[5]

[5] Chapter 11 of [10] discusses the rationale behind some of the P3P vocabulary design decisions in more detail. Certainly these decisions have important implications for both the design of privacy user agents as well as the impacts of P3P adoption; however, a discussion of these decisions and their implications is beyond the scope of this paper.

Complex Privacy Preferences

Surveys have repeatedly shown that most people take a pragmatic approach to privacy, making contextual decisions about whether to protect their privacy or take actions that might put their privacy at risk [1, 25, 26, 39, 43]. Sometimes decisions about whether to provide data are made primarily on the basis of who is asking rather than according to the situation [31]. Furthermore, empirical studies have found that Internet users' behavior is often inconsistent with their self-reported privacy preferences [44]. This suggests that users are willing to make privacy tradeoffs that may be difficult for them to specify in advance. For example, users may have a preference not to have their web browsing activities monitored and profiled. They may feel strongly about this when visiting medical web sites, but they may be willing to allow this monitoring at web sites of book retailers that use this information to make personalized recommendations of books and offer discounts. Indeed some users who otherwise eschew monitoring may even request such monitoring if they find the recommendation service particularly useful.

Inexperienced Users

While most people will readily proclaim a desire for privacy, they usually have little experience articulating a comprehensive set of privacy preferences or rules for a user agent. The task is difficult even when limited to specifying privacy preferences with respect to web site interactions (the only concern of most P3P user agents). Indeed, some have argued that privacy decisions may be too nuanced to be expressed as a set of rules [18].

The task of specifying privacy preferences is further complicated by the fact that discussions of privacy often involve jargon that is understandable only to privacy experts and lawyers. Readability experts have found that the privacy policies on many popular web sites are written at a college reading level or higher [42]. Thus, it is quite understandable that Internet users complain that privacy policies are difficult and time consuming to read [41]. Interface designers are challenged with designing a privacy preference specification interface that uses understandable language and avoids jargon.

Finally, users often do not understand the privacy implications of their online behavior. They may not realize that certain combinations of seemingly non-identifiable information (for example birth date and zip code) might be used to identify them [45]. They also may be unaware of the potential for their computer to be tracked as a result of the IP address that it transmits to web sites. And they may not be able to anticipate in advance when they might want information about their online behavior to remain private. Thus they may be ill equipped to create detailed specifications of privacy preferences.

3. PRIVACY BIRD DESIGN

Our design of the AT&T Privacy Bird interface was informed by our experience with four prototype P3P user agents developed over a four-year period while the P3P specification was evolving [10,48]. In this section we describe our initial public beta release of Privacy Bird as well as a second release made a year later after we made interface improvements following a user study.

Design Overview

AT&T Privacy Bird is a P3P user agent that can compare P3P policies against a user's privacy preferences and assist the user in deciding whether to exchange data with a web site. Privacy Bird is designed as an add-on for the Internet Explorer (IE) 5.01, 5.5, and 6.0 web browsers on Microsoft Windows 98/2000/ME/NT/XP operating systems. Privacy Bird is implemented as a browser helper object [19], which loads whenever IE starts up and runs in the same memory context as IE. We distributed the beta 1.1 and 1.2 versions as free downloads from the http://privacybird.com/ web site beginning in February 2002 and February 2003 respectively. Users download 1.4 MB self-extracting files that include an installation wizard. Once installed, a bird icon with a song bubble appears in the title bar at the top, right-hand corner of the user's Internet Explorer browser windows. The bird changes color and the contents of the song bubble change to indicate whether a web site is P3P-enabled, and (if it is P3P enabled) whether its privacy policy matches a user's privacy preferences.

Users can also click on the bird icon to access additional information about the current web site's privacy policy and the policies that apply to embedded content,[6] as well as configuration and help menus. Figure 3 shows the My Preferences menus and the "green bird" icon that appears when a web site matches a user's privacy preferences. When a user selects the Privacy option from the My Preferences menu, a privacy preference specification interface appears, as shown in Figure 4. This panel allows users to select from high, medium, and low privacy settings; or to customize their settings by selecting up to 12 conditions that should trigger privacy warnings. Users can also import privacy settings (encoded using the APPEL language [14]). We do not display a visual representation of imported APPEL rule sets because imported settings may involve areas not covered by the 12 conditions displayed on this panel.

[6] Embedded content includes images, sounds, frames, and other objects embedded in a web page. Any object that can be addressed by a URL can have a P3P policy.

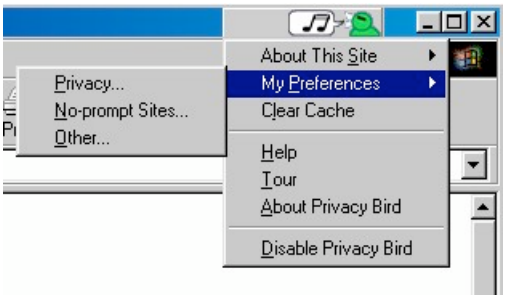

Figure 3. Privacy Bird preferences menu and green bird icon

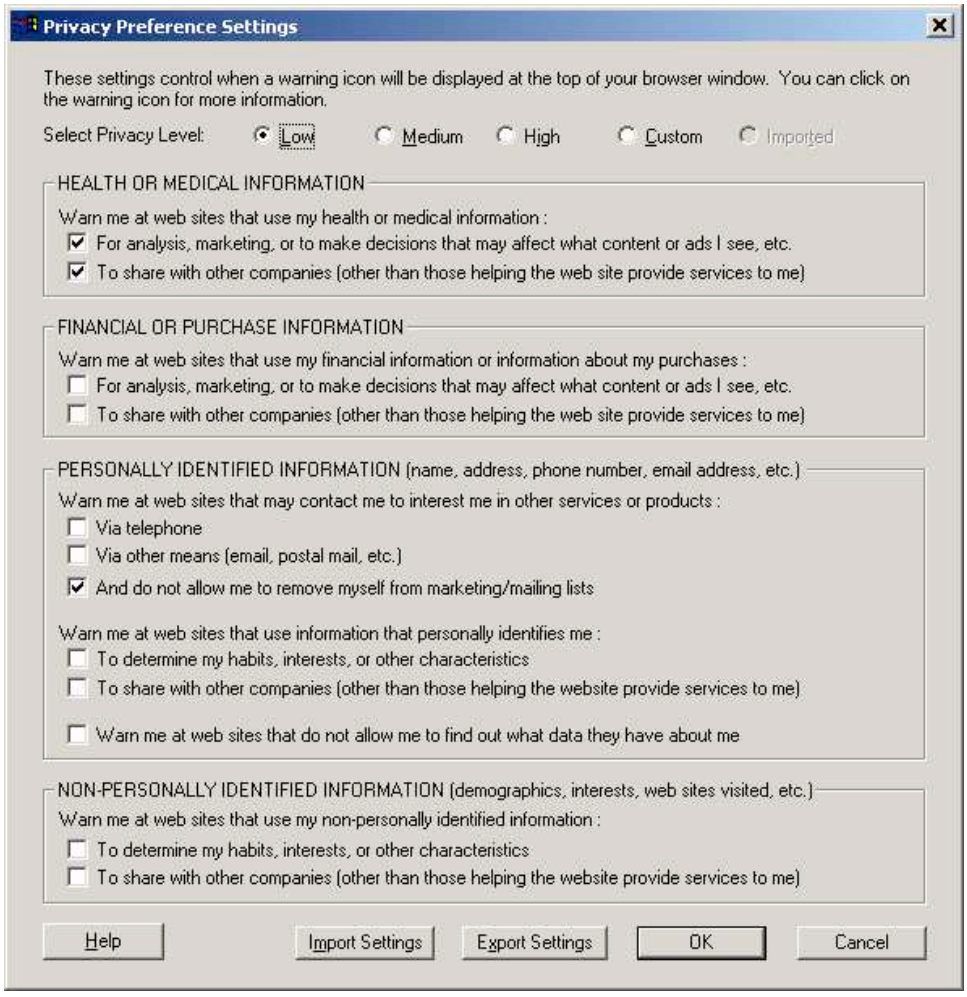

Figure 4. AT&T Privacy Bird privacy preference specification panel

Users can click on the bird icon and select Policy Summary from the About This Site menu to view a summary of the site's privacy policy generated automatically from the site's P3P policy. This summary might be thought of as a privacy "nutrition label."

Figure 5 shows a policy summary for a site that has a policy that does not match the user's preferences. The policy summary begins with a Privacy Policy Check, which indicates the cause of the mismatch. For example, a site's policy might match a user's preferences except for the fact that the site engages in telemarketing. If the site provides a way for users to opt-out of receiving telemarketing solicitations, the policy summary includes a hyperlink that takes users to the opt-out instructions. Below the policy check is a summary derived from the site's P3P policy. It includes a bulleted summary of each statement in the policy, as well as information from the P3P access, disputes, and entity elements, including images of any privacy seals referenced. Rather than using the full definitions of each element from the P3P specification, we developed abbreviated descriptions using plain language. We append the words "unless you opt-out" to those purposes for which an opt-out is available, and provide a hyperlink to the site's instructions for opting out. We append the words "only if you request this" to purposes that occur only if a user opts-in.

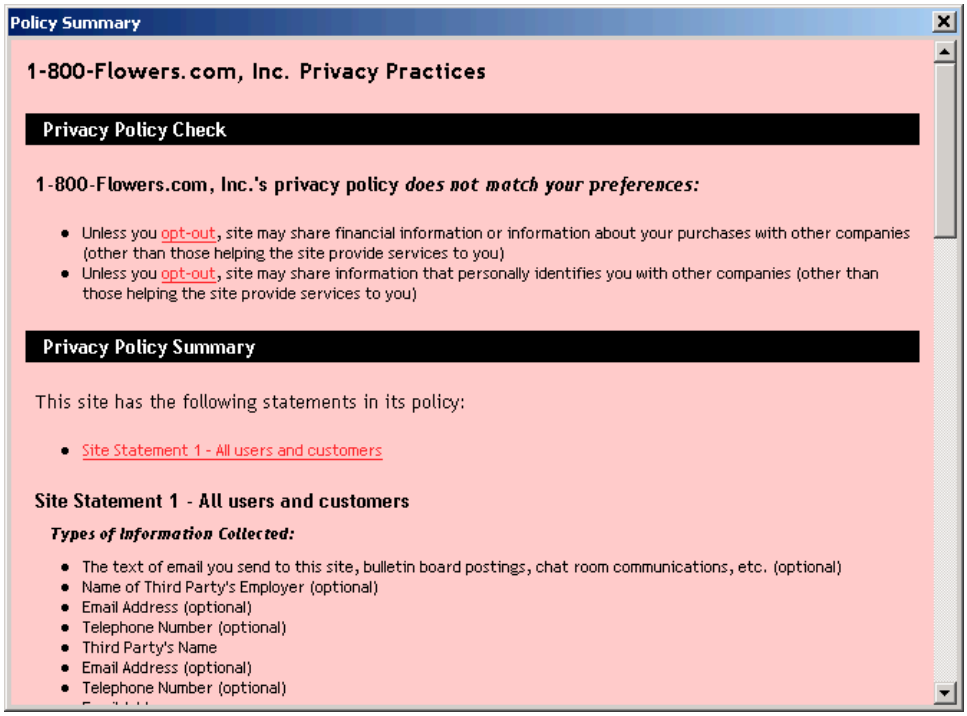

Figure 5. A Privacy Bird beta 1.1 policy summary for a site that does not match the user's preferences

Vocabulary Subset

In order to ease configuration we developed a privacy preference specification interface that would allow users to specify all of their preferences on a single screen, without

having to navigate through multiple levels or tabs, as shown in Figure 4. We wanted users to be able to select a set of data practices about which they would like to receive warnings from Privacy Bird. Clearly representing every possible P3P data practice combination would be impossible, so we reviewed privacy survey results (primarily of American Internet users, as we were designing a user agent with this group in mind) to determine the aspects of privacy policies that would likely be of most interest to users [1, 22, 25, 26]. The three areas that appeared repeatedly as most important were type of data collected, how data would be used, and whether or not data would be shared (represented by the P3P data, purpose, and recipient elements). Among data uses, telemarketing calls and marketing lists seemed to cause greatest concern. Among data types, financial data and medical data appeared to be most sensitive. In addition, individuals did not like having their data used to build profiles of their interests or activities. We focused our configuration interface on these areas of concern. We also decided to include the ability to trigger a warning at sites that have no access provisions because access (also known as individual participation) is a FIP that is getting an increasing amount of attention in the US and is quite important internationally (we discuss the social implications of our choice of vocabulary subset further in Section 6).

It is likely that the choice of what aspects of P3P policies should be highlighted in the user interface will need to be revisited over time and as specialized P3P user agents are developed. For example, although detailed location data such as global positioning system (GPS) data is very sensitive, we did not include a setting that dealt with location data in this interface because Privacy Bird is designed for use on personal computers rather than mobile devices, and thus we do not anticipate that Privacy Bird users will be visiting many web sites that track a user's location. However, as users increasingly use wireless networks to access the Internet from laptop computers, applications that track user location may become more common. Certainly, a P3P user agent for wireless handheld devices should highlight a web site's use of GPS data.

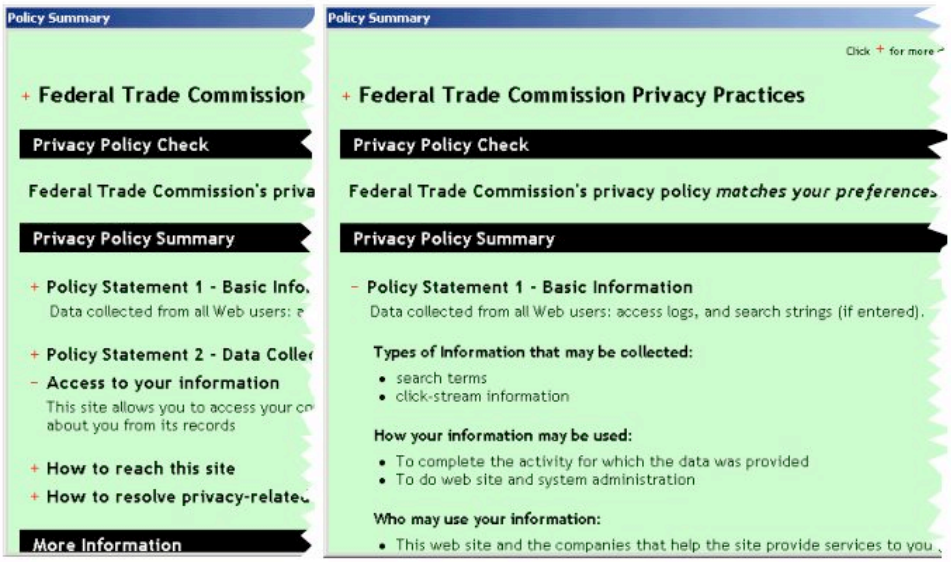

Figure 6. The Privacy Bird beta 1.2 expand/collapse interface. In the policy summary window on the left "Policy Statement 1" has been collapsed. In the window on the right it has been expanded.

In the Privacy Bird policy summary interface we did not display all possible fields available in a P3P policy, but once again focused on those that seemed to raise the most concern for users. In the beta 1.2 release we used an expand/collapse interface to allow users to view P3P policies at varying levels of detail. The plus and minus signs to the left of each heading allowed users to add or hide details, as shown in Figure 6.

Bundling Similar Vocabulary Elements

Many of the distinctions made in the P3P vocabulary are unlikely to be important to most users—although it is quite likely that the distinctions users find most important will change over time and perhaps even vary across regions of the world. We bundled vocabulary elements together that users may think about in similar ways in order to reduce the apparent complexity of the P3P vocabulary. For example, we bundled the six recipients into two groups—sharing, and non-sharing—and described the sharing practice as sharing data "with other companies (other than those helping the web site provide services to me)." Sites that disclose data only to their agents and to delivery companies are considered to be non-sharing, while those that disclose data to any other recipients are considered to be sharing. Thus, P3P vocabulary distinctions between sites that share data with companies having similar privacy policies, companies having different privacy policies, and companies with unknown privacy policies are hidden in the Privacy Bird preference specification interface.

Another bundle we used in the Privacy Bird interface was a set of purposes described collectively as "analysis, marketing, or to make decisions that may affect what content or ads I see, etc." We also used the phrase "information that personally identifies me" to describe collectively three data categories. For P3P experts who want to understand how exactly our bundles map onto the P3P vocabulary, we provide detailed information in the accompanying help files.

We experimented with different bundles in our previous P3P user agent prototypes and refined them after receiving feedback from focus groups and user studies. While our Privacy Bird user studies indicate that our final bundle choices are reasonable, they might be improved further by conducting experiments in which users evaluate bundles independently from the Privacy Bird interface. It would also be useful to verify that our chosen bundles do not serve to confuse or mislead users through groupings that are inconsistent with user expectations.

Removing Jargon

The P3P vocabulary terms borrow terminology from privacy laws and FIPs. While these terms are well known to privacy experts, they are foreign to almost everyone else. Thus it is a challenge for user agent implementers to come up with terms that will be more meaningful to users, while accurately describing the P3P vocabulary.

The P3P vocabulary also uses terms such as "pseudonymous analysis" and "individual decision," which are meaningless without their accompanying definitions, even to privacy experts. Here are the definitions of these terms as they appear in the P3P 1.0 Specification [13]:

> Pseudonymous Analysis: Information may be used to create or build a record of a particular individual or computer that is tied to a pseudonymous identifier, without tying identified data (such as name, address, phone number, or email address) to the record. This profile will be used to determine the habits, interests, or other characteristics of individuals *for purpose of research, analysis and reporting,* but it will not be used to attempt to identify specific individuals. For example, a marketer may wish to understand the interests of visitors to different portions of a Web site.
>
> Individual Decision: Information may be used to determine the habits, interests, or other characteristics of individuals and combine it with identified data *to make a decision that directly affects that individual.* For example, an online store suggests items a visitor may wish to purchase based on items he has purchased during previous visits to the Web site.

These definitions are too lengthy and difficult to understand to be used verbatim in a user interface. We experimented with approaches to describing these purposes that privacy advocates consider to be variations on "profiling." However, the term "profiling" did not

appear to be any more meaningful to most users than the vocabulary terms themselves. From a privacy perspective, it is very important to know that these purposes involve building a record about an individual. However, a description of what the record might be used for seemed to resonate better with users. Ultimately we ended up bundling the profiling purposes with the marketing purposes and some of the most sensitive data groups and the setting became "Warn me at web sites that use my [data category] information for analysis, marketing, or to make decisions that may affect what content or ads I see, etc."

More recently, we have worked with the P3P 1.1 Specification Working Group at W3C to develop "plain language translations" of all P3P vocabulary elements. The following translations have been suggested [46]:

> Pseudonymous Analysis: To do research and analysis in which your information may be linked to an ID code but not to your personal identity.
>
> Individual Decision: To make decisions that directly affect you using information about you, for example to recommend products or services based on your previous purchases.

Using Vocabulary Elements in Combination

In an attempt to simplify the P3P vocabulary, designers might just focus their efforts on bundling elements of the same type together, for example, reducing the number of recipients choices from six to two. However, Internet users tend to have complex privacy preferences that generally cannot be captured by focusing on a single dimension of the P3P vocabulary. It is therefore important that privacy preference options reflect this complexity. For example, we limit warnings about the collection of health and medical information to sites that use this information for purposes that we believe users will most likely find objectionable (marketing, profiling, and sharing with other companies). As a result users should not get warnings at health web sites unless those sites collect health data for one of these objectionable purposes. Indeed eight of our 12 warnings are triggered by a combination of data practices rather than the presence of a single P3P element.

Layered Interfaces

A common way of reducing the complexity of software user interfaces is to divide the interface into two or more layers. Many programs feature configuration menus that include only the most commonly used settings, and a separate "advanced" menu that includes the less frequently used settings. This is an effective way to hide complicated options from users who will never need to access them; however, it sometimes becomes difficult for users who want to access advanced settings to find what they are looking for.

McGrenere, *et al.*, have proposed several variations on the concept of multiple interfaces in which users can select the interface they are most comfortable with and switch between interfaces as needed [34].

Focus group participants that discussed our early P3P user agent prototypes expressed two seemingly contradictory preferences: they wanted the interface to be extremely simple, but they also were reluctant to have their choices reduced to several pre-configured settings such as high, medium, and low. They also expressed concerns about what the default settings would be, a concern echoed repeatedly by privacy advocates [6,27]. We decided to use a layered interface in an attempt to satisfy the preferences expressed by the focus group.

In one of our subsequent prototypes we created three pre-packaged choices, high, medium, and low. These choices were offered on the main configuration screen and more complicated and detailed privacy settings were placed in a separate "custom" control panel. However, because users wanted to learn about the settings behind the pre-packaged settings, this particular approach to layering was not all that effective. Therefore, in the Privacy Bird interface we put the pre-packaged settings in the same window as the custom settings. When a user selects one of the three pre-packaged settings, the boxes next to the corresponding custom settings' warning conditions are checked automatically. (In Figure 4, for example, the "Low" setting has been selected and the three boxes corresponding to that setting are checked.) This provides immediate feedback about what each of the settings does. In addition, it makes it easy for users to make modifications to a pre-packaged setting.

Figure 7 shows how the 12 Privacy Bird Beta 1.2 preference specification options map to the pre-set high, medium, and low levels. These options are represented as a two-dimensional matrix with data types shown across the top and data practices shown down the side. Note that among the data types, the health and financial columns might be thought of as a subset of the personally identifiable information column, although this is not strictly true in all cases. Also, the data practices in the second row are a superset of the data practices in the four following rows. The black areas of the matrix represent combinations of options that are not offered in Privacy Bird beta 1.2. The area labeled region 1 represents the major secondary uses of data, which are captured by the cells surrounding region 3; we offer these options as a package only for the most sensitive types of data for which individuals frequently want to prohibit all secondary uses (preferences regarding less sensitive data tend to be more nuanced). The area labeled region 2 represents options that would allow individuals to specify their preferences

regarding sensitive data in greater detail than we have provided. The area labeled region 3 represents combinations of data practices that cannot occur in practice.

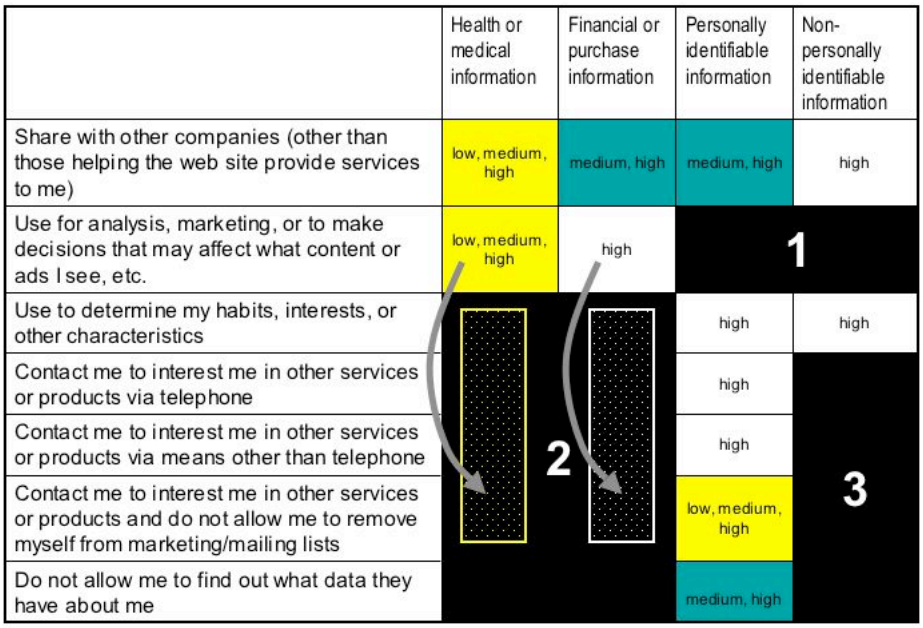

Figure 7. Mapping of preference options to high, medium, and low settings in Privacy Bird beta 1.2. The black areas of the matrix represent combinations of options that are not offered in Privacy Bird beta 1.2. Region 1 represents combinations that are offered only at a more granular level, region 2 represents combinations that are offered only at a less granular level, and region 3 represents combinations that cannot occur in practice.

The choice of which warning conditions to include in each setting was influenced by privacy surveys that have been used to classify individuals into three groups based on their level of privacy concern. These groups include fundamentalists, pragmatists, and individuals who are unconcerned or marginally concerned. While fundamentalists are concerned about a wide range of privacy issues and indicate a willingness to suffer inconvenience and forgo services in order to protect their privacy, the pragmatists are less willing to tradeoff convenience or services to protect their privacy. The marginally concerned expressed concern mostly about protection of their most sensitive data and about privacy intrusions such as junk mail and telemarketing calls [1,25,26]. We designed our settings with these three groups in mind. The design of the high and low settings were fairly straight forward. The high setting triggers warnings for all 12 of the possible warning conditions. The low setting triggers warnings only for the two conditions related to medical data and for the condition triggered by sites that engage in marketing without providing an opt-out. Deciding which triggers to include in the

medium setting was more difficult. We consulted with members of the P3P working group and a number of privacy experts to identify a set of triggers that would likely capture the concerns most important to privacy pragmatists while producing significantly different results than both the high and low settings. Later, a study of 588 P3P-enabled web sites demonstrated that our medium setting does, indeed produce results quite different from the high and low settings. This study found that 25% of sites received red birds on the low setting, 50% of sites received red birds on the medium setting, and 82% of sites received red birds on the high setting [6].

Because of our focus on a subset of the P3P vocabulary, only a small subset of the many possible combinations of user privacy preferences is configurable using the graphical user interface. However, they remain accessible through the APPEL import feature, which adds another layer to Privacy Bird. The APPEL language allows for much more detailed configuration options than most graphical user interfaces can support.

In the beta 1.2 version of Privacy Bird we introduced yet another layering technique by adding buttons in the policy summary to allow users to expand and collapse various components to see more or less detail, as shown in Figure 6. Users wishing to view only a cursory overview of a site's practices might review only the default collapsed view, while user's wishing to view additional details have the option of expanding individual components of the policy summary or the entire policy summary.

Default Settings

Despite our efforts to develop usable configuration interfaces, most users rarely change the default settings on many of the software packages they use. Changing the settings can be time consuming and confusing [32], and users risk "messing up" their settings and being unable to return their software to the state they have grown accustomed to. Designers face choices not only about what the default settings should be, but also when to employ defaults and when to "force" users to make choices [1].

In our design, we tried to avoid setting defaults for the main privacy settings because we wanted users to select settings that would reflect their personal privacy preferences. We wanted to force users to choose the settings themselves; however, we were concerned that it would be difficult for users to make such choices before they had spent time using and understanding the software. So we decided to offer users only the high, medium, and low options during software installation, and make all of the custom options available after the software was installed. However, users complained that they wanted more information about these settings during the installation process. Therefore, in our beta 1.2 release we provided full configuration capabilities (as well as access to all the help files)

during installation. However, users can still select easily between the high, medium, and low options if they do not want to take the time to read and understand the other available options.

Icons and Earcons

Privacy Bird uses icons to provide immediate feedback about whether a site's policy matches a user's preferences. Thus, if a user sees that a policy matches her preferences, in many cases she would not need to look any further. Developing an appropriate icon set and determining where to locate the icon on the screen was a challenge. Other privacy tools have frequently used symbols involving eyes, window shades, and keyholes. Informal feedback and feedback from our focus groups suggested that while these symbols may convey a sense that the tool has something to do with privacy, individuals typically have little idea about what exactly these symbols mean. Furthermore, when designing Privacy Bird we wanted to select symbols that would convey the messages "your preferences are matched" and "your preferences are not matched" rather than "your privacy is protected" and "your privacy is not protected." Thus, we focused on finding symbols that would suggest an agent providing advice. In one prototype we used a thumb's up and thumb's down symbol color-coded with traffic light colors. Our usability test results indicated that this symbol effectively conveyed our intended meaning. However, it appeared that users were relying on the colors more than the symbols, and that they were having difficulties distinguishing the symbol shapes when they appeared as small icons on the computer screen.

When other aspects of our interface design required us to change the shape of the icon from a square to a horizontal rectangle, we revisited the symbol question and came up with the bird symbols (retaining the traffic light colors), as shown in Figure 8. A happy green bird indicates a site that matches a user's preferences, the same green bird with an extra red exclamation point indicates a site that matches a user's preferences but contains embedded content that does not match or does not have a P3P policy, a confused yellow bird indicates a site that does not have a P3P policy, an angry red bird indicates a site that does not match a user's preferences, and a sleeping gray bird indicates that the tool is turned off. The bubbles are designed to be distinguishable by colorblind users and users who do not have color displays. Sounds associated with the red, green, and yellow birds serve to reinforce the visual icons (users can choose whether or not they want to hear these "earcons"). When a user hovers a mouse over the bird icon, a text message explains the meaning of the icon as well.

Figure 8. AT&T Privacy Bird icons

We selected a bird to personify the agent due to some of the images it brings to mind such as "a little bird told me" and a canary in a coal mine serving as an early warning of hazardous gases. More recently sentinel chickens have served as early warning of the West Nile virus, and it has been pointed out to us that a bird was dispatched to determine whether the flood was over in the Biblical story of Noah's Ark. Because the bird symbol does not suggest anything related to privacy, users do not know what it means out of context, and often must read the Privacy Bird tutorial or spend some time using the software before the meaning of the bird symbols are completely clear. However, since Privacy Bird users have to proactively download and install this software, we felt that it was more important that the symbol convey the tool's role as an agent without misleading users into believing that their privacy would be protected for them, rather than conveying that this was a privacy tool. If Privacy Bird were built directly into a browser or other software it would be more important to communicate to users that this symbol was part of a privacy-related feature.

We have received some suggestions for minor changes to the bird artwork to make the bird symbols more easily recognizable on a computer screen. While we have received occasional feedback that the bird is not a serious enough symbol to be used when discussing important privacy concerns, as well as some concerns about slang uses of the term "bird," most of the feedback we have received about our choice of symbols has been positive. In addition, anecdotal evidence suggests that some users are attracted to Privacy Bird because they want to have a "cute" bird in their browser window, and only after downloading the software do they learn about its privacy-related features. Indeed recent studies suggest that users will more readily accept software that triggers positive emotional responses [30].

We decided to locate the bird icons in the top right corner of the browser's title bar for several reasons. First, this enables us to have a separate icon for every browser window a user has open and to have those icons remain visible. Attaching the icon to another part of the browser window (for example in the button area) would cause it to disappear when browser windows are opened as pop-up windows. Placing the icon on a separate tool bar results in a single icon that applies only to the browser window currently in focus (in our beta 1.2 release, in response to user requests, we did end up

introducing an option that allows users to move the bird off the title bar and place it wherever they want on the screen, but this option has the same drawback as the toolbar option). Placing the icon at the bottom of the browser window would result in an icon situated in an area of the screen where most users rarely look [33]. However, this is where the Internet Explorer 6 privacy icon—a do-not-enter sign superimposed on an eye—appears to indicate that cookies have been blocked or restricted.

Some of the most passionate feedback we received about Privacy Bird concerned the earcons that users can configure to accompany the appearance of the bird symbols. While many users found the earcons to be a useful reinforcement for the visual symbols, and some found them to be generally enjoyable, some users complained that they found the earcons extremely annoying. In response to user requests, we introduced an option that effectively results in the sounds being played only once a day at each site a user visits.

In addition to using icons and sounds to provide quick feedback to users, Privacy Bird also displays the Privacy Policy Check section of the policy summary when a user mouses over the red bird icon. This provides immediate feedback about exactly what part of a site's privacy policy conflicts with a user's preferences.

4. OTHER P3P USER AGENTS

We introduce two other P3P user agents here and compare their approach to the privacy preference specification interface and privacy policy summary with our own.

Microsoft Internet Explorer 6

The Microsoft Internet Explorer 6 (IE6) web browser includes cookie management features that allow users to specify cookie-blocking rules based on P3P compact policies. IE6 comes with six pre-configured settings: block all cookies, allow all cookies, high, medium-high, medium, and low [22]. As shown in Figure 9, users can use a slider bar to select their cookie setting and view a short description of each setting. Users can also import custom settings written in a language specified by Microsoft [36]. IE6 comes configured with the medium setting by default.

Like Privacy Bird, IE6 focuses on a subset of the P3P vocabulary, bundles similar vocabulary elements, and uses vocabulary elements in combination. It also provides a layered interface. However, IE6 offers only four P3P-related privacy options to users (unless they import a settings file), while Privacy Bird allows users to select any combination of 12 warning triggers.

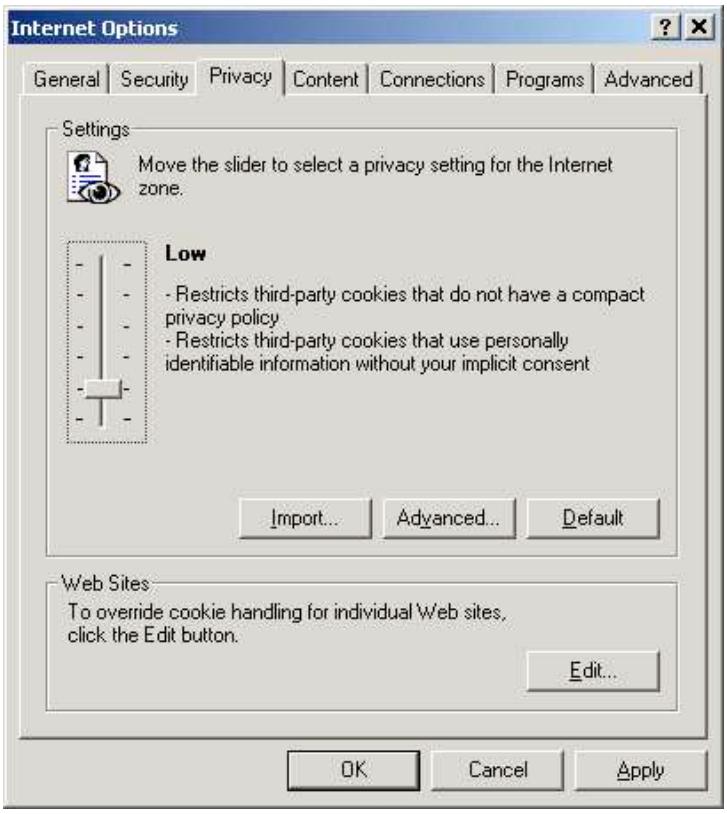

Figure 9. The configuration panel for the Internet Explorer 6 privacy settings.

The IE6 interface includes more jargon than the Privacy Bird interface. For example, the description of the IE6 medium setting includes the following: "Blocks third-party cookies that use personally identifiable information without your implicit consent." Our user studies found that many users were unfamiliar with several of these terms. In addition, in discussions among P3P working group members, even experts have found the phrase "without your implicit consent" confusing.

The IE6 interface also takes a different approach to defaults than Privacy Bird. While some privacy advocates have criticized Microsoft for the default choice of a medium setting, this choice has been especially controversial because it causes many cookies (including all third-party cookies that are not accompanied by P3P compact policies) to be blocked automatically. This, in turn, has been an incentive for web sites to adopt P3P. Privacy Bird does not offer such a direct incentive for P3P adoption.

IE6 offers a "privacy report" similar to the Privacy Bird policy summary. However, the IE6 privacy report is more verbose, providing a paragraph rather than a bulleted item for each P3P element. Unlike the Privacy Bird policy summary, it does not display human-readable elements from the P3P policy. It also omits the required attribute and the

link to the web site's opt-out information (and thus provides no indication about opt-in and opt-out). Probably due to a bug, IE6 displays information about data types only when a web site lists them by category in their P3P policy. If a piece of data is enumerated explicitly (for example, user's first name), IE6 does not mention it at all.

Netscape Navigator 7

Netscape Navigator 7 includes a cookie management feature that allow users to specify cookie-blocking rules based on P3P compact policies that is similar to that found in IE6. The Netscape privacy preference specification interface, shown in Figure 10, uses similar language as the IE6 interface.

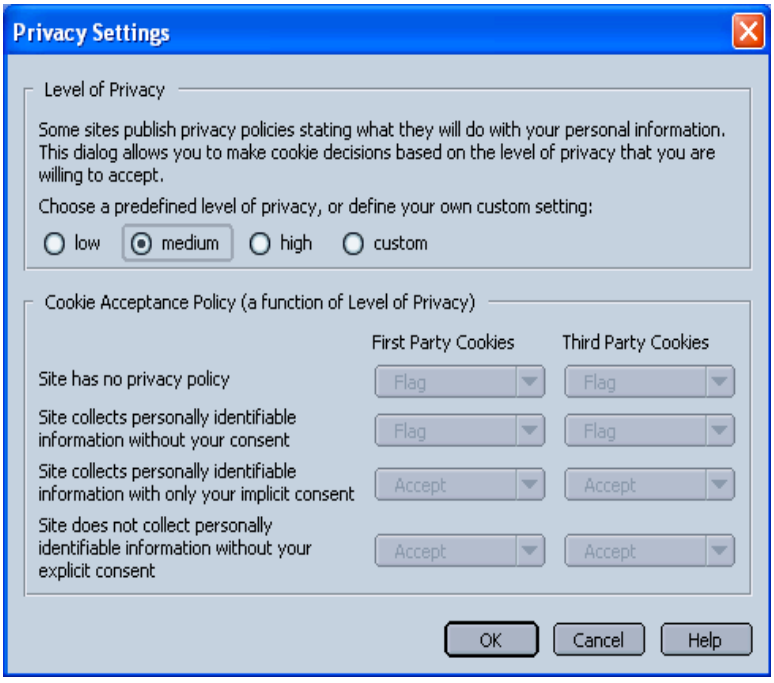

Figure 10. The configuration panel for the Netscape Navigator 7 privacy settings

Like Privacy Bird, the Netscape interface offers pre-packaged high, medium, and low settings that result in the automatic selection of the corresponding custom settings. Also, the Netscape default setting (medium) does not cause cookies to be blocked

Netscape offers a policy summary similar to the Privacy Bird policy summary. It includes a bulleted format, but with different wording than used by Privacy Bird. It also includes a bug similar to the IE6 bug that causes enumerated data not to be mentioned.

5. EVALUATION OF PRIVACY BIRD

A number of criteria might be used to evaluate privacy agents. At a high level, we would like to know whether an agent performs a function that users find useful, and

whether users are able to use the agent effectively. Some P3P critics have argued that for a privacy agent to be effective it must bring about a direct increase in privacy protection for the user through its support of the collection limitation principle. Thus, these critics view software that anonymizes a transaction as an effective PET, but claim that a tool that simply informs users about privacy practices cannot be effective [8,28]. We find this view of PETs to be overly narrow, as increased transparency about privacy practices can enable users to make informed decisions about when to provide their data. As a secondary effect, the transparency provided by the P3P protocol in combination with P3P user agents may motivate web sites to improve the privacy protections they offer, or it may highlight areas where further privacy regulation might be needed [17,37]. Agre suggests evaluation criteria more generally for technical protocols that allow individuals to customize privacy preferences: "These evaluations should employ a broad range of criteria, including ease of understanding, adequacy of notification, compliance with standards, contractual fairness and enforceability, appropriate choice of defaults, efficiency relative to the potential benefits, and integration with other means of privacy protection" [2].

Our focus here is not on evaluating P3P as whole, but on evaluating particular P3P user agents, although we acknowledge that it is not possible to separate the evaluation of P3P user agents completely from a larger evaluation of P3P. We have addressed some of Agre's criteria elsewhere, for example adequacy of notification, contractual fairness and enforceability [16], and compliance with standards [6]. We focus our evaluation here on the usefulness and usability of P3P user agents from the perspective of their users—including issues of ease of understanding and efficiency relative to the potential benefits. In order to evaluate usefulness and usability we study both how a P3P user agent is used in a controlled laboratory setting as well as how it is used in practice. The laboratory study allowed us to make detailed first-hand observations of how first-time users interacted with the Privacy Bird software and to compare Privacy Bird with another P3P user agent. In addition, we were able to observe users performing the same tasks with and without the benefit of a P3P user agent and thus evaluate the effectiveness of the user agent. We also conducted a user survey to gather information about how Privacy Bird is used in practice. This survey provided us with self-reported data from individuals who had been using the software for several months in their own homes or offices.

User Survey

We received informal feedback on our first beta release of Privacy Bird from demo audiences and from some of the approximately 30,000 users who downloaded it. Email from our users focused on requests for new features and ports to other platforms, and

stability and compatibility problems. In order to get additional feedback and gain a better understanding of how people were actually using Privacy Bird we conducted a survey of Privacy Bird users in August 2002. We sent email invitations to complete a 35-question online survey to 2000 of the email addresses provided by individuals who had downloaded Privacy Bird during the first six months of our beta trial and had given their permission to be contacted for user studies. We received 309 completed surveys. We provide an overview of our survey results here; additional details are available in [12].

We asked respondents to evaluate how easy or difficult it was to use several aspects of Privacy Bird. On a 5-point scale (where 1 is very difficult and 5 is very easy) the average rating was 4.6 for installation, 3.9 for changing privacy settings, and 3.3 for understanding the policy summary. As a result we focused most of our attention on improvements to the policy summary for the beta 1.2 release.

A frequent criticism respondents had of Privacy Bird was that a yellow bird appeared at most web sites (because most web sites are not yet P3P-enabled[7] [6]). We asked respondents to predict the usefulness of Privacy Bird if most web sites became P3P enabled. The average usefulness rating on a 5 point scale (where 5 is very useful and 1 is completely useless) jumped from 2.9 for today's web to 4.0 if most web sites were P3P-enabled. Respondents also felt the software would be more useful (4.1) if it was able to block cookies at web sites where the red bird was displayed.

Many Privacy Bird users had strong feelings about the optional sound effects. 45% of respondents reported turning the sounds off completely, while 19% configured Privacy Bird to play sounds at all web sites and 37% configured the software to play sounds only when a certain color bird appeared. Some users praised the sounds but several were quite critical of them. One user complained "damned crow caw really grates on you after a while," and another wrote "I was driven almost to a state of collapse, I used to jump when I heard the same bird call in my yard…." Some users suggested a configuration option in which the bird sound would be played only on the first visit to a particular web site rather than every time a page is loaded.

We asked users whether they had learned anything about web site privacy policies as they used Privacy Bird that caused them to change their online behavior. 88% indicated that their use of Privacy Bird had resulted in some change in behavior. About 37% of respondents reported that they fill out fewer forms online, 37% reported taking advantage of opt-out opportunities, 29% reported that they stopped visiting some web sites, and

[7] In August 2002, Ernst & Young reported that 24% of the top 100 domains and 16% of the top 500 domains visited by US Internet users had been P3P enabled (see

18% reported comparing privacy policies at similar sites and trying to frequent the sites with the better privacy policies. While the fact that these are responses from self-selected survey respondents is probably a factor, these results do suggest that P3P has the potential to influence user behavior.

As a result of this study we made several changes to the Privacy Bird interface before releasing the beta 1.2 version.

Laboratory Study

We conducted a laboratory study involving 12 experienced Microsoft Internet Explorer users who had never used Privacy Bird or the P3P features in IE6. Subjects were given a brief tutorial on Privacy Bird beta 1.2 and the IE6 P3P features and then asked to use these tools to answer several questions about a web site's privacy policy. As a control, they were also asked to read an English-language privacy policy at a different web site and answer the same questions. Subjects filled out pre-test and post-test questionnaires and discussed their experience with a moderator.

We decided to do a direct comparison between Privacy Bird and IE6 rather than Netscape 7 for several reasons. Privacy Bird runs as an add-on to IE6 so we could test both P3P user agents without having to account for different levels of familiarity that subjects might have with the IE6 and Netscape 7 browsers. In addition, IE6 had the highest market penetration of any browser (and thus any P3P user agent) at the time of this study. Finally, Netscape 7's policy summary is more similar to Privacy Bird than is IE6's policy summary, and thus we would expect fewer differences in user responses if we used that as a comparison to Privacy Bird. From discussions with students in an online privacy course who had been assigned to review these user agents as homework, we suspect that the main differences we would find when testing Netscape 7 and IE6 would result from the differences in wording used by these two agents, and the relative location of the menu items. Our students found the Netscape 7 wording overall to be clearer and less verbose than IE6, but found navigating to the P3P-related menu items to be more complicated in Netscape 7. For example, to retrieve the policy summary with Netscape 7 requires a user to select the Page Info option from the View menu, click the Privacy tab, and click the Summary button. In IE6 the policy summary can be retrieved by simply selecting Privacy Report from the View Menu (although anecdotal evidence suggests that very few IE6 users have discovered this menu item). Because IE6 and Netscape 7 have some different features than Privacy Bird (for example, IE6 and Netscape 7 block cookies,

---

http://www.ey.com/global/download.nsf/US/P3P_Dashboard_-__August_2002/$file/P3PDashboardAugust2002.pdf).

while Privacy Bird compares full P3P policies with user preferences), we limited our comparisons to features these user agents have in common.

Methodology

Our subjects were recruited from among employees who work at an office complex in the North Eastern United States. The 12 subjects all had college degrees, and 10 also had post-graduate degrees. They all had jobs that involved a lot of computer work. Their ages ranged from 30 to 52 and they had been using the Internet for an average of 10 years. Seven of the subjects were male and five were female. None had any special expertise related to privacy; however, 11 of the subjects indicated on the pre-test questionnaire that they were somewhat or very concerned about online privacy. In addition, 11 of the subjects said they read privacy policies only occasionally and one reported reading them at most sites where he was considering providing personal information. Subjects were asked to participate in a testing session that lasted approximately one hour and received a token gift as compensation.

The testing was conducted using a personal computer running Windows NT and IE6. Subjects were asked to respond to questions and follow instructions provided by a web-based interface. This interface allowed us to not only record the subjects' responses but also to collect information automatically about how long it took the subjects to perform each task. A moderator observed each test session, verified that the subjects had mastered a set of skills introduced in the tutorial, provided guidance to the subjects when necessary, and asked the subjects some additional questions.

During the training portion of the session, subjects were directed to read tutorial materials provided on the Privacy Bird web site and on the IE6 web site.[8] These materials provide an overview of the functionality of each user agent and specific instructions on configuring each agent and accessing major features. After reading each tutorial, subjects were given a set of tasks to perform. The moderator observed the subjects performing each task and asked them to try again if they did not perform a task correctly. Subjects were also provided with a paper copy of the tutorials to refer to later. All subjects completed the Privacy Bird training before beginning the IE6 training.[9]

[8] The Privacy Bird tutorial is available online at http://www.privacybird.com/tour/1_2_beta/tour.html. The IE6 privacy tutorial is available online at http://www.microsoft.com/windowsxp/pro/using/howto/security/ie6.asp.

[9] We had all subjects complete the training in the same order to reduce the number of variables in our study. However, we discovered that users could better recall what they learned during the second tutorial than the first. We suspect this is due to the order in which the tutorials were presented; however, we have not tested this.

After completing the two tutorials, each subject was asked to perform a set of tasks using Privacy Bird, IE6, and by reading a site's English-language privacy policy. Subjects were randomly assigned an order in which to complete these three sets of tasks. There were six possible orderings of these tasks, and thus two subjects completed the tasks in each order. The tasks involved visiting a specified web site and answering four questions related to the site's privacy practices. All subjects visited the same sites in the same order, regardless of the order in which they performed the tasks. The sites selected were all well-known commercial web sites that had privacy policies that were two to three pages long and P3P policies involving two P3P statement elements. The four questions involved a) determining whether or not the site might send a visitor unsolicited email, b) determining whether or not the site might share a visitor's email address with another company that might send the visitor unsolicited email, c) determining whether or not the site uses cookies, and d) determining what steps a visitor could take to exercise opt-out or unsubscribe options.

Using P3P User Agents to Find Information

Subjects reported that finding information was significantly easier (p-value < .05) using a P3P user agent than reading web site privacy policies. This result is not surprising considering how difficult it is for individuals to read and understand privacy policies [27,41,42]. It would be interesting to repeat this study using particularly well-written privacy policies to see how P3P user agents compare in a "best case" situation. We suspect that P3P user agents would still have an advantage due to the way they standardize the presentation of privacy policies (unless web sites adopt standard formats and wordings for their privacy policies). When using Privacy Bird subjects on average were able to find information slightly faster and more accurately than when reading privacy policies, however, the difference is not statistically significant at the .05 level. Using IE6, subjects actually obtained information more slowly and less accurately than by reading privacy policies; however, they still reported that they found IE6 easier. One of the reasons subjects answered questions incorrectly with IE6 was that IE6 does not distinguish between sites that may send email to all visitors and those that send email only to those who request it. The former sites would be considered to be senders of unsolicited email while the later sites would not. Likewise, using IE6 it is not possible to distinguish between sites that may share data from all visitors with other sites and those that will share data only with a user's permission. If we adjust the accuracy scores to take this into account (by grading the answers based on what IE6 reports rather than on what a site's P3P policy actually says), the average accuracy score for IE6 was not

significantly different from the Privacy Bird accuracy score. The average scores, ratings, and task times are summarized in Table 1.

Table 1. Comparison of Results for Privacy Bird, IE6, and Privacy Policies

	Privacy Bird	**IE6**	**Privacy Policy**
Average number of correct responses to four questions	3.33	2.58 [3.55 adjusted]	3.08
Average time to answer four questions (in seconds)	259	408	285
Average time to answer question 1 (in seconds)	99	162	175
Average time to answer question 2 (in seconds)	61	81	28
Average time to answer question 3 (in seconds)	26	23	19
Average time to answer question 4 (in seconds)	73	142	64
Average rating of ease of finding information on five point scale (where five is very easy and 1 is very difficult)	4.17	2.83	2.08

Several subjects who answered questions incorrectly using Privacy Bird made mistakes because they did not read a particular bulleted item in the policy summary all the way to the end where the phrase "only if you request this" was appended. For example, a site with an opt-in telemarketing policy would have the following phrase in its Privacy Bird policy summary: "To contact you by telephone to interest you in other services or products – only if you request this" It might be helpful to indicate opt-in or opt-out options at the beginning rather than at the end of a bulleted item, or use a change in font color or emphasis to reduce the chance that it will be overlooked.

Examining the task completion times on a question-by-question basis reveals that on average subjects found the answer to the first question significantly faster (p-value = .038) using Privacy Bird than reading privacy policies; however this was not true for subsequent questions. We observed that in the process of answering the questions, most of the subjects read the entire English-language privacy policy in order to answer the first question. After answering the first question, most were able to quickly answer the remaining questions, sometimes without referring back to the privacy policy. When answering the questions with Privacy Bird, most subjects were able to find the answer to the first question without examining the entire Privacy Bird policy summary. Thus, they typically had to refer back to the policy summary in order to answer the subsequent questions. For the last question (finding out how to opt-out), subjects on average

performed significantly worse (p-value < .05) with IE6 than with Privacy Bird or reading privacy policies due to the fact that the IE6 policy summary does not contain the information needed to answer this question without referring back to the English-language privacy policy. Thus subjects who had already spent time reading the policy summary had to then spend time reading the English-language privacy policy. Privacy Bird, on the other hand, provides a link directly to the site's opt-out instructions. This link is actually provided in three places: as a menu option in the Privacy Bird menu, linked from the description of relevant data practices in the policy summary, and in the "More information" section at the end of the policy summary. While most subjects used the link from the end of the policy summary, some took advantage of the other opt-out links.

Although we did not find statistically significant differences overall in the time it took subjects to answer questions with Privacy Bird as opposed to reading a privacy policy, eight of our 12 subjects were able to find information faster with Privacy bird, and we suspect that Privacy Bird users who have gained experience using Privacy Bird could answer these questions significantly faster than those using it for the first time. We observed that some subjects initially went to the preference configuration screen rather than the policy summary to try to find information, and others went to the policy summary but initially looked at the wrong parts of the privacy summary to find the requested information. Since all subjects read the Privacy Bird tutorial prior to reading the IE6 tutorial, their Privacy Bird training was not fresh in their minds when they began answering questions with Privacy Bird, even if they were given the Privacy Bird tasks prior to the other sets of tasks. Indeed several subjects remarked that they had confused the Privacy Bird and IE6 instructions, and that they felt Privacy Bird would get easier to use over time. To provide some data to support our speculation that over time users would be able to find information faster with Privacy Bird, we recruited eight additional subjects for a short test. Half of the subjects received Privacy Bird training and were asked to answer our set of four questions at two web sites using Privacy Bird. The other half were asked to answer our set of four questions at two web sites by reading those sites' privacy policies. All subjects visited the same two sites but we varied the order in which they visited them. The four subjects who used Privacy Bird all found the information faster at the second site (average = 163 seconds) than the first (average = 214 seconds), with no significant differences in the accuracy with which they answered the four questions. We found the most significant time differences for the first question, which took subjects an average of 101 seconds to answer at the first site and 63 seconds to answer at the second. Of the four subjects who read the privacy policies two found information faster at the first site and two found information faster at the second site (this

was not dependent on which site they visited first), with no significant differences in the accuracy with which they answered the questions. On average these subjects found information in 329 seconds at the first site and 303 seconds at the second site. It would be interesting to try a similar experiment with experienced Privacy Bird users and with individuals who reported frequently reading privacy policies to investigate this learning effect over a longer time period.

We asked five additional sets of questions in the post-test questionnaire in order to compare users' attitudes about Privacy Bird and the IE6 P3P features. We asked users to rate on a 5-point scale (where 5 is more favorable than 1) the usefulness of each tool, how likely they would be to use it in the future, how likely they would be to recommend it to a friend, how easy it was to understand the policy summary information provided by each tool, and how easy it was to find the information we requested using each tool. For each question Privacy Bird received significantly higher average ratings than IE6 (p-value < .005 for all questions except the second, which had p-value = .032), as shown in Table 2. While we must consider the possibility that subjects may have been biased by knowledge that Privacy Bird was developed by AT&T (which conducted the study and employed most of the subjects), our observations of the subjects' behavior while using the two P3P user agents is consistent with the ratings they provided. For example, many subjects remarked that they liked the structured nature of the Privacy Bird policy summary and found the bulleted items easy to read and understand. They liked the fact that Privacy Bird presents information in a consistent format, and criticized English-language privacy policies for being verbose, convoluted, and not formatted in a standard way. They also remarked that although the IE6 policy summary uses a standard format, they found it to be far too verbose, which made it difficult to quickly scroll through it to find particular information. Some subjects used the browser's search feature to attempt to find information in the English-language privacy policies. They usually had to try several terms until they figured out what terminology a particular web site was using to describe a given data practice, and sometimes this strategy proved ultimately unsuccessful. The subjects who used this search strategy when examining the English-language policies expressed a desire to use this strategy to find information in the IE6 policy summary; however, no search facility is provided.

Table 2. Average Ratings of Privacy Bird and IE6 on a Five-Point Scale Where 5 is More Favorable Than 1

	Privacy Bird	**IE6**

Usefulness	4.17	3.25
Likely to use in the future	4.60	3.50
Likely to recommend to a friend	4.58	2.75
Ease of understanding policy summary	4.00	2.67
Ease of finding information	4.17	2.83

Information Presented by P3P User Agents

While there is much overlap between the types of information presented in the IE6 and Privacy Bird policy summaries, there are some differences. IE6 presents information on web site data retention policies, while Privacy Bird does not. Privacy Bird presents information about opt-in and opt-out choices and displays the human-readable consequence field that allows sites to provide summary information about each of their P3P statements. In the beta 1.2 version of Privacy Bird used in our study, the Policy Summary displays the consequence fields when a user first accesses it and hides several other fields. Users can use the expand/collapse feature to view the rest of the fields. In addition, Privacy Bird displays information about specific data elements a site collects if the site provides it, while IE6 provides only information about the categories of information a site collects. There are some fields in a P3P policy that neither user agent displays to users.

We observed that the expand/collapse function was not completely intuitive to all our subjects. While all eventually figured out how to use it, some spent a lot of time looking for information during the training tasks before they realized they could click on the plus sign to find it. A more obvious mechanism for activating this functionality would be helpful, perhaps buttons labeled "show details" and "hide details." In addition, it would be useful to highlight this feature in the Privacy Bird tutorial (it is currently not mentioned). Nonetheless, once they figured out how to use it, several subjects took advantage of this feature.

We asked our subjects several questions in an attempt to gauge whether Privacy Bird was displaying the right quantity and type of information to users. In our pre-test questionnaire we asked subjects to tell us about their personal privacy preferences at web sites. Ten subjects said they did not want sites to share their personal data, three said they did not want to receive unsolicited email, two said they did not want their data to be used for a purpose other than the purpose for which it was provided, and two said they didn't want sites installing unwanted software on their computers. With the exception of

the last item (which is not addressed by P3P policies) the Privacy Bird policy summary provides information relevant to all of these preferences.

In our post-test questionnaire, 11 of our subjects said that amount of information displayed by Privacy Bird was "about right" and one said it was "too much." When we had previously asked respondents in our user survey what additional information they would like included in the policy summary, none of them had an answer, so in this study we asked subjects specifically about whether they would like to see information about a site's data retention policy added. Eight subjects said they would like to see this information, but only three said it was as important as the information already included in the policy summary. This suggests that in the future P3P user agent designers should consider including this field in the information they provide to users, but that it need not be featured prominently (in our expand/collapse interface, we would probably have this information collapsed by default).

After discussing the possibility of adding information about data retention to the policy summary we asked our subjects if there was anything else we should add. Several said there was nothing they wanted added but they would like to see some information highlighted at the top. In particular, they mentioned wanting to know whether their data would be shared and whether or not they would receive unsolicited marketing communications. This is consistent with the preferences our subjects conveyed in the pre-test questionnaire. Although this information is included in both the IE6 and Privacy Bird policy summaries, users have to check the appropriate sections of each of the statement elements in a site's policy in order to find it. While the sites subjects visited in our study each had only two statements, many web sites have policies with considerably more statements. This information would be more accessible if aggregated across all of the statements and highlighted at the top of the policy summary. Other suggestions for information to add included information about exactly which companies might receive their data, an automatic opt-out link that didn't require filling out a form, more information about the consequences of providing information to a web site, and information about whether the site would attempt to put spyware on the their computer. Although all of these items are beyond the scope of what can be expressed in a P3P policy, they still might be implemented in a privacy user agent. The fact that the P3P vocabulary cannot address all of these issues might be viewed as a shortcoming of P3P itself, although it might also be argued that these issues would best be addressed by complementary mechanisms rather than by broadening the scope of P3P.

Icons

We asked our subjects some questions in our pre-test questionnaire to gauge the intuitiveness of the Privacy Bird and IE6 privacy icons. About half of our subjects were able to correctly determine the meaning of all of the Privacy Bird icons with the exception of the icon depicting the green bird with an exclamation point (which only two subjects identified correctly). Only three of our 12 subjects were able to correctly determine the meaning of the IE6 icon that appears when cookies have been blocked or downgraded. Some subjects said they were confused because it was not immediately clear to them that the Privacy Bird icons represented birds. After reading the Privacy Bird tutorial, none of our subjects had difficulties determining the meanings of the Privacy Bird icons. However, some commented that they would like to see a bird that looked more bird-like. Some of the subtle things we did to reinforce the meaning of the different icons proved more distracting then helpful, for example, some subjects complained that the symbols used in the birds eyes made the birds look less bird-like without conveying obvious meaning. On the other hand, several subjects commented positively on the bird sounds, which they said helped reinforce the meaning conveyed by the visual icons. In addition, several subjects commented that they liked the fact that the bird icon was always present on the screen, and some speculated that once they became more familiar with the preference settings they would be able to determine whether sites would share their data or send them unsolicited email simply by looking at the bird icon and noting whether or not it indicated that the site's policy matched their preferences.

Those subjects who identified Privacy Bird icons incorrectly typically suggested a literal meaning of the icon—for example, the singing bird might indicate a site that plays music, and the swearing bird might indicate that a site uses foul language. The yellow bird with the question mark evoked a different kind of confusion. Some subjects correctly determined that this icon indicated that there was something unknown or confusing about the site. However, others focused on the color scheme and concluded that the yellow bird indicated that the site wasn't good enough to receive a green bird but wasn't bad enough to receive a red bird. Whether sites that are not P3P-enabled should be considered better or worse than those that are P3P-enabled but have unacceptable policies is a debatable question. By assigning sites with unknown policies a yellow bird we convey the message that users should be cautious when visiting these sites, but that they aren't as bad as sites that have red birds. Arguably, to promote P3P adoption it would be better to assign these sites a symbol that users would interpret as worse than the symbol assigned to sites that do not match their preferences. However, users might find this approach discouraging while the majority of sites they visit are not P3P-enabled.

Privacy Bird does not take steps to protect privacy directly; it simply provides a visual indicator that allows users to make more informed privacy-related decisions. As discussed in Section 3, we attempted to convey this idea through our choice of an icon that avoids use of more typical symbols associated with privacy. Anecdotal evidence from our user study suggests that users did understand this. However, it would be useful to conduct a study that would directly probe whether Privacy Bird users hold misconceptions about the ability of the tool to directly protect their privacy.

Language used in Preference Configuration Interface and Policy Summary

Much of our previous design work on P3P user agent prototypes focused on refining the wording of the preference configuration interface and policy summary. Based on this experience we selected some of the terms that we expected to be most problematic and included questions in our pre-test and post-test questionnaires designed to assess our subjects' comprehension of these terms. This was by no means a comprehensive assessment of the terminology used in P3P user agents. In addition, our very well educated subjects may have found this terminology less confusing than less well educated subjects might.

The meaning of the "ours" recipient element is difficult to convey to users. The element is intended to convey that a site is generally using data internally without sharing it. However, sites may correctly declare this element if they share data with "agents" that use it only on behalf of the site and for the purpose for which it was provided. While it is tempting to simplify this term and simply tell users that data is not being shared, this is an over simplification that can be misleading. In addition, as we have learned from our previous prototypes, any terminology that uses the term "agent" tends to be confusing to users who aren't sure what exactly an agent is in this context. This point was driven home to us when we had subjects test our previous prototype by visiting a P3P-enabled web site for a real estate broker. When we asked subjects to read the policy summary and tell us with whom the site would be sharing data, several subjects had responses that indicated they believed the word "agent" in this context referred only to real estate agents.

In our post-test questionnaire we showed subjects three phrases describing the ours element, as shown in Figure 11. (The source of these three phrases was not revealed to our subjects.) Subjects unanimously identified the new alternative as the clearest, and suggested only a few minor changes to improve it further. They liked the fact that this wording avoids the use of jargon and includes concrete examples.

IE6: Information may be used by this web site, entities for whom it is acting as an agent, and/or entities acting as its agent. An agent in this instance is defined as a third party that processes data only for the completion of the stated purpose, such as a shipping firm or printing service.

Privacy Bird: Information may be used by this web site and the companies that help the site provide services to you (such companies must use your information only on behalf of this web site for the purposes stated in this policy).

New alternative: Information may be used by this web site and the companies that help the site fulfill your requests (for example, shipping or billing companies -- such companies may not use your information for marketing or other purposes that go beyond fulfilling your request).

Figure 11. Three alternative wordings to describe the P3P "ours" recipient element

In order to assess the ability of users to comprehend the terms used in the preference configuration interfaces of Privacy Bird and IE6 we showed subjects these interfaces set at their respective "low" settings (shown in Figures 4 and 9) and asked subjects to describe each setting in their own words. All subjects were able to correctly describe the Privacy Bird low setting. However, most subjects were unable to correctly describe the IE6 low setting. The terms "third-party cookie" and "compact policy" were unknown to most subjects. In addition, most were unable to figure out what "implicit consent" means, especially when used in the phrase "without your implicit consent," which some interpreted as a double negative but they weren't sure what was being negated. IE6 uses the terms explicit and implicit consent to refer to opt-in and opt-out respectively. All subjects were able to correctly explain the meaning of opt-in and opt-out but most were unsure of the meaning of implicit consent and explicit consent.

Privacy Agents as Educational Tools

In our post-test questionnaire we asked subjects whether they would be more likely, less likely, or just as likely to read privacy policies after participating in our study. Eleven of our 12 subjects said they would be more likely to read privacy policies. This is especially interesting considering that these subjects had not previously expressed an exceptional interest in privacy policies and were unaware that they would be doing tasks related to privacy policies when they volunteered to participate. These results suggest the potential of using P3P user agents as educational tools. Some of the respondents to our user survey and participants in our previous studies had suggested this as well. Indeed, other privacy agents have been developed explicitly for this purpose. Alsaid and Martin have suggested adding P3P functionality to their "Bugnosis" tool, which is designed to educate policy makers and journalists about web bugs [3].

In the future we might look for ways to take this idea further by providing short educational modules or privacy "tips" that users have the option of accessing as they use Privacy Bird. Such modules might provide more information on topics such as how cookies work, how web sites can link together data to identify an individual, and the potential privacy implications of various activities. Another possible approach would be to use a critic-based architecture that prompts users with suggested changes to their settings periodically as they use the software [11].

6. CONCLUSIONS

In this paper we have discussed PETs, P3P, and the AT&T Privacy Bird user interface. We have highlighted several design approaches that we found useful and believe may have utility in future privacy agent interface development efforts.

Summary of Findings and Future Work

Our evaluations indicate that overall users find Privacy Bird to be both useful and usable. We have identified a number of areas where improvements might further increase usefulness and usability, including highlighting important issues in the policy summary, improving some of the wording, refining the Privacy Bird icons, and providing a more obvious expand/collapse mechanism. Our policy summary format with short bulleted items was much more appealing to users than the verbose paragraphs used by IE6. Users also indicated that they liked having a persistent privacy icon that gave them immediate information about whether a site's policy matched their preferences, and they found it useful to be able to determine why they were receiving privacy warnings.

Our efforts to focus on a subset of the P3P vocabulary, bundle similar vocabulary elements, and use vocabulary elements in combination appear overall to be effective. More work is needed to determine whether our choices of bundles and combinations can be further improved, or whether any of these simplifications risk misleading or confusing users.

Our evaluations demonstrate that users appreciate short summaries of privacy information, as long as they do not hide critical information. Standardized formats allow users to find the information of most interest quickly. Users are not familiar with much of the terminology used by privacy experts, so it is important to use words and phrases that will be meaningful to them. Future P3P user agents should highlight data sharing and marketing practices, as well as opt-out information. Summary information may combine information about multiple aspects of privacy or reduce the granularity of information if this will help users understand the information being conveyed to them or allow them to

more easily make configuration decisions. These findings might be applied to the development of future privacy agents, as well as other types of PETs, and even to the design of written privacy notices.

The results of our evaluations have already influenced the development of the draft P3P 1.1 Specification, which includes a set of plain language translations of P3P policy elements [46]. Our user studies have highlighted the importance of standard formats and language in the presentation of privacy policies, and have provided insights into how to phrase descriptions of privacy concepts in ways that will be comprehensible to users.

In the future, Privacy Bird might be expanded to include a more explicit privacy education component and to keep track of what information users have provided to each web site and the privacy policy under which each piece of information was provided. Privacy Bird might allow users to establish a number of personae and, in the words of Burkert, "help us remember whether, when, and towards whom, on the Internet, we had been a dog or a cat" [5]. In addition, since completing our Privacy Bird evaluations we have developed a prototype search engine front end that incorporates Privacy Bird, thus enabling users to compare web sites easily on the basis of their privacy policies and to identify sites that match their personal privacy preferences [7].

More detailed preference specification interfaces may be needed as privacy agents are developed that take actions beyond providing information to users. Future P3P user agents may be bundled with other types of PETs that may block cookies, anonymize data, or otherwise limit collection or use of data. In a P3P user agent that blocks cookies or takes other actions, users may need to make other decisions such as what types of cookies to block (first-party, third-party, session, etc.), whether to turn persistent cookies into session cookies, and whether to make decisions based on cookie-specific privacy policies or privacy policies for the broader web site. Analyses of previous versions of browser cookie interfaces have found them to be inadequate [35], and from the difficulties we observed users having in interpreting the IE6 preference configuration screen it is clear that further work is needed to develop effective cookie interfaces.

As privacy agents are built to help users manage control of their data by electronic wallets, single-sign-on services [40], and new applications facilitated by web services, the semantic web [4], and ubiquitous computing environments [21,29], it will be important that users are able to effectively use these agents. Services are emerging that will make it more convenient for users to engage in online transactions without the need to repeatedly authenticate themselves and type in address, payment, and other information. In the longer term we may see customized services that can take advantage of information about a user's schedule, location, characteristics, and preferences. If users delegate decisions

about the release of their personal information to automated agents, it will be critical that these agents have user interfaces that allow users to clearly specify the conditions under which their data should be released. Our work offers a step towards gaining an understanding of how to develop such interfaces; however, additional research is needed.

Social Implications

It has been suggested that we "regard PETs as a technical innovation to help us to solve a set of socio-political problems" [5], and P3P, in particular, has been described as a "social protocol" [15]. Thus it is important to consider their social implications. Tools such as Privacy Bird that focus on informing users have the potential to increase transparency associated with privacy practices and in turn serve as a catalyst for companies to improve these practices. Agents that take actions such as blocking cookies or controlling access to an electronic wallet may have even more direct influence on privacy practices. Already we hear of companies changing their policies so as to avoid having their cookies blocked by IE6. The aspects of privacy policies that designers choose to highlight in user interfaces thus play a role in influencing future policy decisions. Designers have an opportunity to build interfaces that will reinforce the status quo or attempt to push generally accepted business practices in a direction that is more privacy friendly. For example, a designer might decide not to highlight the access provisions of a privacy policy due to the fact that access does not appear to be one of the higher priorities for users. On the other hand, companies have not been too eager to inform their customers about access provisions and access is not something that most individuals have come to expect (in the US at least). However, access is a fundamental FIP principle, and user agent designers have an opportunity to promote the provision of access by highlighting it in their interfaces. There is also a danger that privacy agents may serve to reinforce the acceptability of marginal privacy provisions or lead to user complaisance. Users may believe that their privacy agent is providing protections that it is incapable of providing, or protections that are not provided under the default settings. Or users may believe incorrectly that the configuration options presented by the agents reflect the entire range of privacy practices that might be provided. Returning to the access example, if access is omitted from configuration choices it may not even occur to some users that it might be possible for them to gain access to their own information.

As we have discussed throughout this paper, balancing the desires of keeping interfaces simple with providing flexibility and educating users about privacy is a complicated problem to solve. It is important that designers of privacy agents are cognizant of the social implications of their designs, and consider these implications from

the beginning of the design process [20]. Designers of privacy agents have enormous opportunities as well as great challenges to overcome.

7. ACKNOWLEDGMENTS

Thanks to the anonymous reviewers for their many useful suggestions. Thanks also to Ellen Isaacs and John Baldasare for assisting with the design and testing of our previous P3P user agent prototypes on which the design of Privacy Bird was based, to Gary Zamchick for designing the Privacy Bird icons, and to Michael Zalot for designing the Privacy Bird earcons.

8. REFERENCES

1. Ackerman M.S., Cranor, L.F., and Reagle, J. Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences, in Proceedings of EC'99 (Denver CO, November 1999), ACM Press, 1-8.
2. Agre, P. 1997. Introduction. In P. Agre and M. Rotenberg (eds.) *Technology and Privacy: the New Landscape*. MIT Press, Cambridge, MA.
3. Alsaid, A., and Martin, D. 2002. Detecting Web Bugs with Bugnosis: Privacy Advocacy through Education. In *Proceedings of the 2002 Workshop on Privacy Enhancing Technologies (PET2002)*. http://www.cs.uml.edu/~dm/pubs/bugnosis-pet2002.ps.
4. Berners-Lee, T., Hendler, J., and Lassila, O. May 2001. The Semantic Web. *Scientific American.*
5. Burkert, H. 1997. Privacy-enhancing technologies: typology, critique, vision. In P. Agre and M. Rotenberg (eds.) *Technology and Privacy: the New Landscape*. MIT Press, Cambridge, MA.
6. Byers, S, Cranor, L., and Kormann, D. 2003. Automated Analysis of P3P-Enabled Web Sites. In *Proceedings of the Fifth International Conference on Electronic Commerce (ICEC2003)*. Pittsburgh, PA, October 1-3, 2003.
7. Byers S, Cranor, L., Kormann, D., and McDaniel P. 2004. Searching for Privacy: Design and Implementation of a P3P-Enabled Search Engine. In *Proceedings of the 2004 Workshop on Privacy Enhancing Technologies (PET2004)*. Toronto, Canada, 26-28 May, 2004.
8. Catlett, J. Open letter to P3P developers & replies. In Proceedings of CFP2000 (Toronto Canada, April 2000), ACM Press, 157-164.
9. Cranor, L. 1999. Internet Privacy. *Communications of the ACM 42,* 2, 29-31.
10. Cranor, L. *Web Privacy with P3P.* O'Reilly & Associates, Sebastopol CA, 2002.
11. Cranor, L. and Ackerman, M. Privacy Critics: UI Components to Safeguard Users' Privacy, in Proceedings of CHI'99, short papers (Pittsburgh PA, 1999) ACM Press, v. 2, 258-259. Available at http://lorrie.cranor.org/pubs/privacy-critics.pdf.
12. Cranor, L. Arjula, M., and Guduru, P. 2002. Use of a P3P User Agent by Early Adopters. In *Proceeding of the ACM workshop on Privacy in the Electronic Society*. 1-10.
13. Cranor, L., Langheinrich, M., Marchiori, M., Presler-Marshall, M., and Reagle, J. The Platform for Privacy Preferences 1.0 (P3P1.0) Specification. World Wide Web Consortium Recommendation, April 2002. http://www.w3.org/TR/P3P/.
14. Cranor, L., Langheinrich, M., and Marchiori, M. A P3P Preference Exchange Language 1.0 (APPEL1.0). World Wide Web Consortium Working Draft, April 2002. http://www.w3.org/TR/WD-P3P-Preferences.
15. Cranor, L. and Reagle, J. 1998. Designing a Social Protocol: Lessons Learned from the Platform for Privacy Preferences Project, in J.K. MacKie-Mason and D. Waterman (eds.) *Telephony, the Internet, and the Media.* Lawrence Erlbaum Associates, Mahwah, NJ. http://www.w3.org/People/Reagle/papers/tprc97/tprc-f2m3.html
16. Cranor, L. and Reidenberg, J. 2002. Can user agents accurately represent privacy notices? *TPRC 2002*. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=328860
17. Cranor, L. and Wenning, R. 2002. Why P3P is a Good Tool for Consumers and Companies. *GigaLaw.com*. http://www.gigalaw.com/articles/2002/cranor-2002-04.html
18. Dourish, P. 2004 Security as Experience and Practice: Supporting Everyday Security. Talk delivered at the Workshop on Usable Privacy and Security Software, Rutgers, NJ. July 8, 2004. http://www.ics.uci.edu/~jpd/talks/wupss-security.pdf
19. Esposito, D. Browser Helper Objects: The Browser the Way You Want It, MSDN Library, January 1999. http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwebgen/html/bho.asp.

20. Friedman, B., Kahn, P., and Borning, A. 2002. Value Sensitive Design: Theory and Methods, UW CSE Technical Report 02-12-01, http://www.ischool.washington.edu/vsd/vsd-theory-methods-tr.pdf.
21. Gandon, F.L. and Sadeh, N.M. (2003) *A Semantic e-Wallet to Reconcile Privacy and Context-awareness.* In *Proceedings of the Second International Semantic Web Conference (ISWC03)*.
22. Georgia Tech Graphics, Visualization & Usability Center. GVU's 10th WWW User Survey, 1998. Available at http://www.gvu.gatech.edu/user_surveys
23. 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.
24. Goldfeder, A. and Leibfried, L. Privacy in Internet Explorer 6. MSDN Library, October 2001. http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnpriv/html/ie6privacyfeature.asp.
25. Harris, Louis and Associates and Westin, A.F. Harris-Equifax Consumer Privacy Survey 1991. Equifax Inc., Atlanta GA, 1991.
26. Harris, Louis and Associates and Westin, A.F. E-commerce & Privacy: What Net Users Want. Privacy & American Business, Hackensack NJ, 1998.
27. Hochhauser, M. 2003. Why Patients Won't Understand Their HIPAA Notices. Privacy Rights Clearinghouse. http://www.privacyrights.org/ar/HIPAA-Readability.htm.
28. Hochheiser, H. 2002. The platform for privacy preference as a social protocol: An examination within the U.S. policy context. ACM Transactions on Internet Technology, 2, 4, 276-306.
29. Hull, R., Kumar, B., Lieuwen, D., Patel-Schneider, P., Sahuguet, A., Varadarajan, S., and Vyas, A. Enabling Context-Aware and Privacy-Conscious User Data Sharing. In Proceedings of the 2004 IEEE International Conference on Mobile Data *Management*.
30. Khong, P., and Song, J. 2003, Exploring user's emotional relationships with IT products: a structural equation model, in *Proceedings of the 2003 international conference on Designing pleasurable products and interfaces,* ACM Press, 45-50.
31. Lederer, S., Mankoff, J., and Dey, A. 2003. Who Wants to Know What When? Privacy Preference Determinants in Ubiquitous Computing. In *Proceedings of the conference on Human factors in computing systems*. 724-725.
32. Mackay, W.E. 1991. Triggers and barriers to customizing software, in *Proceedings of CHI'91*, ACM Press, 153-160.
33. McCarthy, J.D., Sasse, A.M., and Riegelsberger, J. 2003. Can I have the menu please? An eyetracking study of design conventions. To be presented as a Full Paper at HCI2003, University of Bath, 8th - 12th September 2003.
34. McGrenere, J., Baecker, R., and Booth, K. 2002. An evaluation of a multiple interface design solution for bloated software, in *Proceedings of CHI'2002*, ACM Press, 164-170.
35. Millett, L., Friedman, B., and Felten, E. 2001. Cookies and Web browser design: toward realizing informed consent online. In *Proceedings of the SIGCHI conference on Human factors in computing systems*. 46-52.
36. MSDN Library, How to Create a Customized Privacy Import File. 2002. http://msdn.microsoft.com/library/default.asp?url=/workshop/security/privacy/overview/privacyimportxml.asp.
37. Mulligan, D., Cavoukian, A., Schwartz, A., and Gurski, M. 2000. P3P and Privacy: An Update for the Privacy Community. http://www.cdt.org/privacy/pet/p3pprivacy.shtml
38. Organization for Economic Co-operation and Development. (1980) *Recommendation Of The Council Concerning Guide-Lines Governing The Protection Of Privacy And Transborder Flows Of Personal Data.* Adopted by the Council 23 September 1980. http://www.datenschutz-berlin.de/gesetze/internat/ben.htm
39. Palen, L. and Dourish, P. 2003. Unpacking "Privacy" for a Networked World. In *Proceedings of the conference on Human factors in computing systems.* 129-126.
40. Pfitzmann, B. and Waidner, M. 2002. Privacy in browser-based attribute exchange. In *Proceeding of the ACM workshop on Privacy in the Electronic Society*. 52-62.
41. Privacy Leadership Initiative. Privacy Notices Research Final Results. Conducted by Harris Intereactive, December 2001. http://www.ftc.gov/bcp/workshops/glb/supporting/harris%20results.pdf.
42. Rodger, W. Privacy Isn't Public Knowledge: Online policies spread confusion with legal jargon, USA Today, 1 May 2003, 3D. Available at http://www.usatoday.com/life/cyber/tech/cth818.htm.
43. Sheehan, K.B. 2002. Toward a Typology of Internet Users and Online Privacy Concerns. *The Information Society, 18,* 21-32.
44. Spiekermann, S., Grossklags, J., and Berendt, B. E-Privacy in 2nd Generation E-Commerce: Privacy Preferences versus actual Behavior, in Proceedings of EC'01 (Tampa FL, October 2001), ACM Press, 38-47.
45. Sweeney, L. Information Explosion. In L. Zayatz, P. Doyle, J. Theeuwes and J. Lane (eds), *Confidentiality, Disclosure, and Data Access: Theory and Practical Applications for Statistical*

Agencies. Urban Institute, Washington, DC, 2001. http://privacy.cs.cmu.edu/people/sweeney/explosion.html

46. Wenning, R., ed. The Platform for Privacy Preferences 1.1 (P3P1.1) Specification. W3C Working Draft 27 April 2004. http://www.w3.org/TR/2004/WD-P3P11-20040427/
47. Whitten, A. and Tygar, J.D. 1999. Why Johnny can't encrypt. In *Proceedings of the 8th USENIX Secrutiy Symposium*.
48. World Wide Web Consortium. FTC Comment: Script of W3C P3 Prototype. June 1997. http://www.w3.org/Talks/970612-ftc/ftc-sub.html