Global Information Assurance Certification Paper

P3P –A Case of Privacy Smoke and Mirrors

Darrell M. Mills
March 31, 2002
GSEC Version 1.3

Abstract

Many users have expressed a great deal of distrust and unwillingness to use the Internet for transacting business and exchanging personally identifiable and financial information. Lack of strong legally enforceable data privacy rules, as well as confusing and inconsistent practices by organizations with an online presence, are a main reason.

This paper will discuss a technical privacy solution currently being proposed called P3P or Platform for Privacy Preferences Project. It will present an overview of what P3P is, and why the current implementation has generated a great deal of discussion on both sides of the privacy debate, questioning whether P3P improves Internet privacy or gives users a false sense of security. We will be defining P3P and its relationship to cookies and then review the current P3P implementations in Microsoft Explore 6.0 and the AT&T Privacy Bird application. Next, we will address acceptance of the P3P standard by nations/unions other than the United States. Finally, we will look at the baseline that P3P is referencing, the privacy policy. Our question is, even if we have an effective P3P product and implementation, can the user be assured that their personally identifiable information is protected?

Introduction

In a recent article in Computerworld, Patrick Thibodeau writes on how U.S. corporations are facing continuing if not greater resistance from the American public regarding their distrust of current corporate privacy policies. According to Thibodeau, "the most recent piece of evidence of customer mistrust was offered in a poll conducted by Rochester, N.Y. – based Harris Interactive for Privacy & American Business, a nonprofit think tank in Hackensack N.J.; Ernst & Young International in New York; and the American Institute of Certified Public Accountants in New York. The poll of 1,529 adults found that 75% believed that their information would be shared without their permission, and 69% felt that hackers could steal their data. [10] In another article, Thibodeau states that an e-mail poll taken last summer by the Gallup Organization, a think tank in Princeton, N.J., found that 80% of 400 users said they are "very concerned" about misuse of credit card data on the internet. In a study by Cambridge Mass. – based Forrester Research Inc., it was estimated that if it wasn't for privacy concerns, total online spending last year of $47.6 billion would have been $15 billion higher. [11]

This issue doesn't only affect the American public. Since the Internet is truly an international medium of communication and commerce, the privacy standards and regulations of many countries and political unions factor in, particularly, how personally identifiable information is used and to whom it is disclosed. Public disclosure of these practices in the form of the organization's privacy policies online has been treated differently by nations around the world. The result has been inconsistency and at times outright confusion for the user. Solutions to these problems have spanned the spectrum

from legislation to technology to self-regulation. Due to the divergent interest of the consumers of Internet services and those who provide Internet services, including Internet advertisers and marketing groups, the solutions may not be that clear or easily agreed upon.

P3P Defined

The Platform for Privacy Preferences (P3P) is an emerging Web standard, developed by the World Wide Web Consortium (W3C), a coalition of industry and nonprofit groups, organized to develop interoperable technologies including specifications, guidelines, software and tools for the Web. As defined by the W3C:

> P3P 1.0 creates the framework for standardized, machine-readable privacy policies, and consumer products that read these policies. Web sites express their privacy policies in a simple standardized format that can be downloaded automatically and read by web browsers and other end-user software tools. These tools can display information about a site's privacy policy to end users, and take actions based on a user's preferences. Such tools might provide positive feedback to users when the sites they visit have privacy policies matching their preferences, and provide warnings when a mismatch occurs. They may also notify users when a site's privacy policy changes.[12]

Implementation of P3P requires two important components: the web site software and the browser client agent. To deploy P3P to the web site, first we need to create an appropriate policy statement, identifying what data the site collects and how this data will be used. These policy statements are then converted into machine-readable XML documents for publishing on the Web site.

Then we create a policy reference file as an XML document to be published, with the URL referencing the site's policy statements. The reference file lists the P3P policies used by the site. It also indicates that part of the Web site and Web site's cookies, which are covered by the policy statements. A human readable version of the site's privacy policy must be available on the Web site. At the same time that the machine-readable XML version is published, the human readable version must be published with a link pointing to it from the policy statement. An HTTP response header sent by the server, or a link in the site's HTML may indicate the reference file's location. The preferred method is to place the policy reference file in a well-known location. Automated tools may be used to make this process much simpler.

Browser software can include the client agents to automatically get and read the Web sites P3P privacy policies. The client agents can be included with the browser, as in the case of Internet Explorer 6.0 or implemented through plug-ins, browser helper objects, proxies, or other application software, as with the AT&T Privacy Bird application. A P3P enabled browser can obtain the Web site's machine-readable privacy policy automatically and notify the user of the Web site's information privacy practices according to the browser side preference implementation of the P3P client.

The development of consumer products to use this framework can be implemented through various applications. The W3C developed the standard with flexibility, as a way to support a wide range of user preferences, public policies, service provider policies and applications. Their expressed intent was to focus on improving Internet privacy, user confidence and trust.

As a note of caution, the P3P standard is only a framework specification for development of privacy preference tools. **These tools currently only warn the user or block certain cookies if the Web sites policies differ from their list of preferences.** It is not based on a regulatory requirement for protection of individual privacy rights. It depends on self-regulation by the Web site provider. It is only a standard protocol for exchanging policy statements and preferences. Furthermore, Web sites have the option whether to incorporate the P3P protocol into their sites or may choose not to because they have collected too much information, considered it too costly, or just decided it to be unnecessary. If too few sites support P3P, consumer use will be minimal and marketers will most likely not bother to implement it.

The Role of Cookies

Since HTTP is referred to as a "stateless protocol," each request for a web page is an independent transaction; nothing links one request to another. [3] In answer to this, cookies were developed as a way to "tag" the user's browser with information. The information is then stored in a cookies folder on the user's hard drive. This simple exchange and storage of information made it easier for users to access their favorite Web sites without having to re-identify themselves. Web sites also use cookies to track what the user requests from the site and to recognize the user's computer when the user makes future requests.

The kinds of information contained in a typical cookie file may include: a unique serial number assigned to the user which can be used to reference the user in the site's databases, number of times the site has been accessed, the first and last times accessed, the pages accessed and much more. Cookies are also used for web site personalization, where an individual profile is created for the user. This profile is built by combining the cookies' identifying information with off-line databases containing personal information about the user, such as credit card numbers, mailing address, phone numbers, household incomes and personal preferences for products or services. [5]

One of the largest users of cookie technology is the Internet advertising industry. Advertising networks, like DoubleClick, Engage, the Flycast network and MatchLogic, include their banner advertisements on a majority of the most popular sites on the web. [5] Matchlogic alone maintained a profile database of more than 72 million anonymous users. [9] Unknown to most Internet users is the degree to which these companies are creating large databases to record who looks at what web pages. In December 1998, DoubleClick placed 48 million cookies on users systems. The trend has been for these Internet advertising companies to "synchronize" their online profiles with offline direct marketing databases. The result is to create a fairly accurate picture of the online behavior of readily identifiable individuals.[5]

Cookies provide beneficial functionality to Web applications, allowing Internet users to easily connect with, request and process transactions online. Yet this functionality has bred an undesirable potential for abuse through the collection, processing, access and sharing of an individual's personally identifiable information, without their expressed approval. Does P3P in any way give us control on how cookies are used? Maybe we can get a better idea by looking at the Microsoft and AT&T implementations using the P3P standard.

The Microsoft P3P Implementation

In mid-March of 2001 Microsoft announced that it would include key features of the P3P specification in the next versions of its Web browser software, Internet Explorer 6.0 and, at the same time, MSN would also create and implement privacy statements on its sites. [7] Rick Belluzzo, president and chief operating officer at Microsoft, said, "With these significant privacy features in Internet 6.0, Microsoft is helping to give people critical notice and consent information in their browser experience, to better know what information is collected about them via cookies." In addition, Belluzzo stated that, "Privacy is a key part of Microsoft's .NET efforts, and this work is a step toward enabling the .NET experiences of the future, where devices, applications and services work together on behalf of the users." [8]

Microsoft's implementation of the P3P specification involved the summarization and representation of policy information in regard to the site's use of cookies in what Microsoft called a compact policy or CP. The CP is actually a single line description of the site's privacy policy and is contained in the HTTP header information. This information includes XML tags for data, recipient and purpose. [8] This puts the emphasis of Microsoft's P3P implementation on cookie management.

A part of the cookie management is cookie filtering. Internet Explorer 6.0 determines what action to take based on the context in which the cookie was sent and the content of the cookie CP. Internet Explorer 6.0 will then accept, deny or downgrade the cookie. Down graded cookies are deleted after the browsing session ends or the cookie expires. If the CP detects that a cookie, related to a P3P specified personally identifiable information element, is used for a secondary purpose or outside of the CP-stated purpose, without allowing user choice of opt-in or opt-out, the cookie is considered unsatisfactory. The following is a list of the P3P personally identifiable information elements:

- **CON**. Information regarding contact or location.
- **ONL**. Online information regarding contact or location, such as e-mail address.
- **GOV**. Information regarding identification issued by the government such as Social Security number.
- **FIN**. Information regarding personal finances.

As mentioned above, a cookie used for a secondary purpose refers to the use of the information that goes beyond the user's specific intent, when they provide the personally identifiable information. Elements defining secondary usage are:

- **SAM.** Personally identifiable information that may be shared with other parties with similar privacy practices.
- **DEL.** Used for delivery purposes beyond the user's original intent.
- **OTR.** Information shared with parties accountable to the provider, but may use the information in an undisclosed manner.
- **UNR.** Provider of the information is not aware of how the information will be used.
- **PUB.** Full public distribution of Information.
- **CUS.** User-requested site modifications.
- **IVA.** Individual user specific analysis.
- **IVD.** User history based actions.
- **CON.** Individual contact information.
- **TEL.** Information obtained for telemarketing purposes.
- **OTP.** Any other purpose not mentioned by the above P3P purposes.

The user can set their privacy preferences, relative to the Web sites' cookie usage and compact policy (condensed computer readable privacy statement) regarding first and third party web site usage, of the personally identifiable information. A first-party Web Site is the one that is currently being viewed. A third-party Web site is any other one than the one currently being viewed. Third party sites sometimes include their content along with the first party site. An example of this is a third party Web site providing advertising content through inclusion of their cookies.

To set or change the privacy preferences, users can go to the Tools tab on the Internet Explorer 6 tool bar and select the Internet Option tab, and then the Privacy tab. A window with a slider should appear. Below are listed the six privacy levels on the Privacy Tab window slider bar, which filters both the Web site's cookies, and in some cases, looks for the sites compact policy (CP):

- **Blocks All Cookies -** All cookies are blocked and cookies already on your computer cannot be read by any Web sites.
- **High -** Cookies will be blocked from all sites that do not have a compact policy and from those sites that use personally identifiable information without the user's explicit consent.
- **Medium-High -** Cookies will be blocked from all sites that do not have a compact policy and from those sites that use personally identifiable information without the user's explicit consent. First party sites that use personally identifiable information without the user's implicit consent will have their cookies blocked.
- **Medium (default) -** Cookies will be blocked from all sites that do not have a compact policy and from those sites that use personally identifiable information without the user's explicit consent. First party sites that use personally identifiable information, without the user's implicit consent, will have their cookies deleted from the user's computer when the user closes Internet Explorer.

- **Low -** Cookies will be blocked from all sites that do not have a compact policy. Third party sites that use personally identifiable information, without the user's implicit consent, will have their cookies deleted from the user's computer when the user closes Internet Explorer.
- **Accept All Cookies -** All cookies are allowed and will be stored on the computer. Cookies currently existing on the user's computer can be read by those Web sites that created them. (This is the setting most common on the Web today).

The Microsoft P3P implementation deals mainly with cookie management and cookie filtering. By itself IE 6.0 appears to too confusing and complex. It is also questionable whether most users will configure the software's preferences for their best protection.

The AT&T P3P Implementation

Another example of a P3P implementation is AT&T's Privacy Bird software, which is a tool that can be added to the Microsoft Internet Explorer Web Browsers (versions 5.01/5.5/6.0). This software is a browser add-on, which searches for privacy policies at every site visited. A wizard helps the user configure personal preferences, and a drop-down menu is available to update these when necessary. [1] Rather than just cookie management, as in Microsoft's implementation, AT&T's implementation allows the user to specify a number of specific choices such as:

Health or Medical Information

- Warns the user of web sites that use their health or medical information to perform analysis, marketing, or for making decisions that may affect what content or ads the user sees.
- Warns the user of Web sites that share their health or medical information with other companies. This may include companies who work with the Web site in providing services to the user.

Financial or Purchase Information

- Warns the user when connecting to Web sites that employ the user's financial or personal information regarding purchases to perform analysis, marketing, or for making decisions. These may affect what content or ads the user sees.
- Warns the user when connecting to Web sites that share their financial or personal information regarding purchases with other companies. This may include companies who work with the Web site in providing services to the user.

Personally Identifiable Information (name, address, phone number, email address, etc.)

- Warns the user when connecting to Web sites that may:
    - Contact them by telephone, email, postal mail or any other means them to interest them in other services or products.
    - Not allow them to remove themselves from marketing/mailing lists.
- Warns the user when connecting to web sites that use information that personally identifies them to determine their habits, interests, or other characteristics.
- Warns the user when connecting to Web sites that share personally identifiable information with other companies. This may include companies who work with the Web site in providing services to the user.

- Warns the user when connecting to Web sites that do not allow them to find out what data the site has about them.

Non-Personally Identifiable information (demographics, interests, web sites visited, etc.)

- Warns the user when connecting to Web sites that use their non-personally identifiable information, to determine their habits, interests, or other characteristics.
- Warns the user when connecting to Web sites that share non-personally. identifiable information with other companies. This may include companies who work with the Web site in providing services to the user.

Once the privacy preferences are set, the Privacy Bird can trigger warnings for sites whose published policies use the above mentioned preferences, contrary to what was selected. Differences in privacy preferences can be viewed in a summary window. An option at the end of the summary allows the user to view the site's full privacy policy. There is a window the user can select to "Opt-In/Opt-Out" of inclusion in the mailing list, or the marketing of services and products. Finally, another window can be selected to view a list of all images and other files that are embedded in the web page currently being visited.

As a technical specification for privacy protection, the Microsoft and AT&T implementations attempt to satisfy the requirement in different ways. The Microsoft implementation uses cookie management with cookie filtering based on privacy preference. The AT&T implementation automatically reads full P3P privacy policies and displays them to the user. In addition, AT&T's' Privacy Bird allows a variety of customization options based on personal privacy concerns. When used together, the Microsoft and AT&T products offer a more robust tool set for displaying information to the user regarding the site's privacy policies, and whether those policies match their personal privacy preferences or not.

Acceptance of P3P In Countries With Strong Privacy Standards

The European Union (EU), through the EU Data Directive, provides a baseline of legally enforceable privacy rights. The European Commission, which reviews and recommends policy to EU members, gave an opinion on including P3P as part of their privacy protection framework. In this opinion, the commission rejected P3P based on the numerous problems it found with the protocol. They stated that, "Surprisingly, given the intention that P3P be applicable worldwide, the vocabulary has not been developed with reference to the highest known standards of data protection and privacy, but has instead sought to formalize lower common standards." [4] The commission pointed out that if P3P were to provide the required support for privacy protection on-line, the use of a technical platform for privacy protection would not of itself be sufficient to protect privacy on the Web.

They went on to emphasize that the technical platform cannot operate alone, but must be applied within the context of a framework of enforceable data protection rules or statutory regulation. At a minimum, these rules must provide a non-negotiable level of

privacy for all individuals. The opinion was careful to emphasize that use of P3P without this framework of enforceable data protection rules, could potentially shift the primary responsibility of privacy compliance from the Web site providers to the users themselves. This would conflict with what they referred to as an internationally established principal that it is the "data controller" (Web site provider) who is responsible for complying with data protection principles. In the view of the EU, such a reversal of responsibility would impose upon the individual user, a level of knowledge regarding data processing risks, which in itself would not be reasonable to expect of the average citizen.

As a part of this argument, the EU further described a potential risk where upon inclusion in future versions of Internet browsers, P3P could actually mislead EU-based Web site providers into assuming that they have met their legal obligations regarding the granting of access to user data. This applies if the individual user agrees to this part of the site's privacy policy in the online negotiation. The opinion stated that the actions of these Web Site Providers must follow the requirements of EU data protection directives, as stated in their national laws in the collection, processing and granting of access to any personal data. Therefore it would be essential that in the implementation of P3P, any confusion be avoided between the Web site providers and their legal obligations and the Internet users and their data protection rights. This pertains to the design and configuration of browsing software distributed and sold in EU ensuring that the online privacy agreements are not in contradiction with current data protection laws.

In view of these issues, and the fact that P3P is currently seen as a substitute for privacy protection law rather than a component of statutory privacy protection, its adoption by the EU and similar communities with strong legally enforceable privacy rights with may be a ways off.

Then there is the privacy policy, the baseline that P3P is referencing. With the most effective P3P products and implementation of the P3P framework, we are still only exchanging machine-readable information on the Web site's privacy policy. What value is P3P if the site's policies cannot be trusted? Can the user be assured that their personally identifiable information is protected? Can the ability of the Web site to self-regulate and audit itself be a major weakness? Is there an independent verifying authority attesting to the Web site's privacy practices? These are interesting questions, since according to the Harris Interactive survey, some 84% of the 1,529 people surveyed said they would like checks and balances via "independent verification" of company's privacy policies. [6] Would this improve user confidence and trust? To answer these questions, let's see whether organizations that grant privacy seals through independent verification can address this.

Privacy Policies and Privacy Seals

As an attempt to self-regulate, the Internet and data marketing industries have developed their own voluntary enforcement mechanism, through the use of privacy seals.

BBB Online and TRUSTe Privacy Seals

The seals or "trustmarks" shown above, when displayed on a web site, indicate that the site adheres to the letter of their published policy. In order to display the seal, the site will pay an annual licensing fee, and allow the licensing organization to evaluate their privacy practices. Those sites, which are licensed by TRUSTe, are reviewed periodically by "seeding " their sites' databases with traceable information. BBB Online, on the other hand, requires its member sites to perform an annual self-assessment by answering a number of questions on privacy practices. Both BBB Online and TRUSTe have a dispute resolution process, which allows the user to address violations of privacy policy. [5] For those cases where their disputes are not resolved, the sites may lose their seals and the cases may be referred to government prosecutors as possible fraud cases.

A verification process as described above might be fine, if it worked. In a paper written in February 2000, Christopher Hunter described the ordeal a customer would go through to pursue a complaint against a Web site. He noted that a speedy resolution is not that easy to obtain. The example was given of TRUSTe, a licensing organization who grants privacy seals to member businesses, requiring users to first complain to the offending Web site. If the response was not prompt or was unsatisfactory to the consumer, TRUSTe would step in. TRUSTe would then decide whether the complaint was valid. If TRUSTe found the complaint worth pursuing, it would attempt to negotiate a settlement between the Web site and the consumer. In the case a satisfactory solution is not reached, TRUSTe will then call in outside auditors. Then finally and only in "extreme cases," TRUSTe will forward the complaint to the "appropriate government agency." [5] Hunter goes on to say that "Yet even more troubling than this burdensome resolution process, is the fact that TRUSTe has repeatedly found ways to allow member web sites to wiggle out of their contractual obligation, to abide by their posted privacy policies." [5]

The fact that this happens shouldn't be surprising. A report from Forrester Research, a research firm whose business is to advise companies, was highly critical of self-regulation. According to Forrester, "because independent privacy groups like TRUSTe and BBB Online earn their money from e-commerce organizations, they become more of a privacy advocate for the industry – rather than for consumers. The FTC should call for a consumer-based organization to provide principles and redress." [2] Jason Catlett of Junkbusters put it simply by saying "This make as much sense as putting the Fortune 500 companies in charge of setting taxation policy for the IRS, and for running its compliance division." [2]

So what value is P3P if the sites policies cannot be trusted? It doesn't appear the P3P is of much value if we cannot trust the Web sites policies. Can the user be assured that their personally identifiable information is protected? No, without the trust, there is no

assurance of protection. Can the ability of the Web site to self-regulate and audit itself be a major weakness? Absolutely, without trusted third party verification through an independent audit, we have a major weakness. Is there an independent verifying authority attesting to the Web site's privacy practices? No, right now the verifying organization's customers are the people who they are auditing and being paid by. It looks like privacy seals haven't helped too much in improving Internet privacy, user confidence and trust. With a lack of independence and over reliance on self-regulation, the Web sites may virtually sign off on the audit process and declare them selves in full compliance with their privacy policies, whether they are or not.

Issues with P3P

From this discussion, I think we have some clear issues with P3P as a viable framework for data privacy. These issues include:

As a standard protocol for exchanging policy statements and preferences, it adds confusion and complexity. For the average Internet user, the P3P framework appears very confusing and adds a level of complexity with very little benefit in providing additional protection of individual privacy rights. This is particularly true when it comes to configuring their browsers to best protect their personal data.

Organizations can choose whether or not to participate (no full participation required). Without full participation by Web site providers, users are not likely to accept it and marketers will not implement it. Full participation is necessary for fair disclosure of Web-based privacy practices.

There will be no assurance to users that the Web sites will follow published policies. If there is no assurance that the Web sites will adhere to their published policies, P3P will further erode the Internet user's level of confidence and trust in dealing with Web site providers. Further confusion will only complicate efforts to establish effective privacy controls for individuals.

No valid independent audit of sites privacy practices. Without truly independent audits of these Web sites' compliance to their published policies and privacy practices, P3P will have minimal following.

No strong legislation, requiring adherence to standard privacy practices on the collection, processing, access to and sharing/disclosure of personal identifiable information. The primary attributes that we are lacking which other countries have developed are strong privacy regulations with a baseline of legally enforceable privacy rights. It's evident that without strong privacy legislation, Internet users will have great difficulty in fully embracing the Web as a safe and secure medium for personal information.

Conclusion

As a privacy enforcer, P3P fails. As a standard protocol for exchanging policy practices and preferences, it's still too complex. If Web site providers can choose whether or not to participate, and the only penalty for not participating is the disapproval of the marketplace, there will be no assurance to users of the privacy of their personal data. Lacking strong privacy legislation, requirements for fair disclosure and full participation by all the Web site providers, statutory regulation (not self-regulation) and truly independent audit of compliance to published policies and privacy practices; we are at present facing a false sense of security. I think the jury is still out on this one. This appears to be a case of privacy smoke and mirrors, but with the implementation of strong and legally enforceable privacy rules, along with standard worldwide protocols agreed upon by all nations/unions, the Internet could be a reliable and secure medium for transacting business for all users.

Internet Resources

1. AT&T. "Privacy Bird - Privacy Preference Settings"
URL: http://www.privacybird.com/help/help-privacypreferencesettings.html (18 March 2002).

2. Catlett, Jason. "Profiling Comments to the Dept. of Commerce and Federal Trade Commission." (October 1999).
URL: http://www.ftc.gov/bcp/profiling/comments/catlett.htm (18 March 2002).

3. Electronic Privacy Information Center. "Pretty Poor Privacy: An Assessment of P3P and Internet Privacy." (June 2000).
URL: http://www.epic.org/reports/prettypoorprivacy.html (12 March 2002).

4. European Commission. "Platform for Privacy Preferences and the Open Profiling Standard. Draft opinion of the Working Party on the Protection of Individuals with regard to the processing of Personal Data." (January 1998).
URL: http://www.epic.org/privacy/internet/ec-p3p.html (18 March 2002).

5. Hunter, Christopher. "Recoding the Architecture of Cyberspace Privacy: why Self-Regulation and Technology Are Not Enough." February 2000.
URL: http://www.asc.upenn.edu/usr/chunter/net_privacy_architecture.html (3 March 2002).

6. Johnson, Maryfran. "Follow the (Privacy) Money" (February 2002).
URL: http://www.computerworld.com/storyba/0,4125,NAV47_STO68536,00.html (18 March 2002).

7. Microsoft. "Microsoft P3P Implementation In Internet Explorer 6.0 and Windows XP Fact Sheet."
URL: http://www.microsoft.com/presspass/press/2001/mar01/PrivacyToolsIEfs.asp (18 March 2002).

8. Microsoft. "Microsoft to Deliver on Privacy Tools in Internet Explorer."
URL: http://www.microsoft.com/presspass/press/2001/Mar01/03-21PrivacyToolsIEPR.asp (18 March 2002).

9. Saunders, Christopher. "MatchLogic Faces Privacy Suit." November 2000.
URL: http://www.internetnews.com/IAR/article/0,,12_518201,00.html (12 March 2002).

10. Thibodeau, Patrick. "Corporate Privacy Credibility Crumbles." March 2002.
URL: http://www.computerworld.com/storyba/0,4125,NAV47_STO68778,00.html (19 March 2002).

11. Thibodeau, Patrick. "The Roots of Mistrust Go Deep." (March 2002). URL; http://www.computerworld.com/storyba/0,4125,NAV47_STO68779,00.html (4 March 2002).

12. W3C Platform for Privacy Preference Initiative. "An Introduction to P3P." URL: http://www.w3c.org/P3P/introduction.html (3 March 2002).