DOWNLOAD PDF P3P HISTORY ; P3P-ENABLING YOUR WEB SITE : OVERVIEW AND OPTIONS

Chapter 1 : PPT - Deploying P3P on Web Sites PowerPoint Presentation - ID

P3P: Introduction 2 P3P history P3P: Enabling your web site - overview and options. 11 21 Enabling your web site - overview and options 34 P3P Policies.

Tuesday, December 7, 5: However, project presentations will be scheduled during our final exam slot. All students are expected to attend. Final project papers are due December 13 at noon. Your final grade in this course will be based on: Class discussions will often be based on these assignments and you will not be able to participate fully if you have not done the reading. It is suggested that you write up summaries and highlights as you read each chapter or paper and bring them with you to class. All homework assignments must be typed and submitted in hard copy in class on the day it is due. Every homework submission must include a properly formatted bibliography that includes all works you referred to as you prepared your homework. These works should be cited as appropriate in the text of your answers. All homework is due at the beginning of class on the due date. I reserve the right to take off additional points or refuse to accept late homework submitted after the answers have been discussed extensively in class. Reasonable extensions will be granted to students with excused absences or extenuating circumstances. Please contact me as soon as possible to arrange for an extension. Cheating and plagiarism will not be tolerated. Students caught cheating or plagiarizing will receive no credit for the assignment on which cheating occurred. Additional actions -- including assigning the student a failing grade in the class or referring the case for disciplinary action -- may be taken at the discretion of the instructor. A class mailing list has been setup for announcements, questions, and further discussion of topics discussed in class. Students will be expected to contribute to mailing list discussions. Students should post non-personal course-related questions to this mailing list rather than sending them to the instructor directly. Students are encouraged to post course-related items of interest to this mailing list.

DOWNLOAD PDF P3P HISTORY ; P3P-ENABLING YOUR WEB SITE : OVERVIEW AND OPTIONS

Chapter 2 : Online Privacy Issues Overview

2 Privacy Policy, Law and Technology â€¢ Carnegie Mellon University â€¢ Spring â€¢ 3 Lorrie Cranor â€¢ www.nxgvision.com

Edit As the World Wide Web became a genuine medium in which to sell products and services, electronic commerce websites tried to collect more information about the people who purchased their merchandise. Users who saw this as an invasion of privacy would sometimes turn off HTTP cookies or use proxy servers to keep their personal information secure. P3P is designed to give users a more precise control of the kind of information that they allow to release. P3P manages information through privacy policies. When a website uses P3P they set up a set of policies that allows them to state their intended uses of personal information that may be gathered from their site visitors. When a user decides to use P3P they set their own set of policies and state what personal information they will allow to be seen by the sites that they visit. As an example, a user may store in the browser preferences that information about their browsing habits should not be collected. If the policy of a Website states that a cookie is used for this purpose, the browser automatically rejects the cookie. The main content of a privacy policy is the following: The location of the XML policy file that applies to a given document can be: However, the P3P functionality in Internet Explorer extends only to cookie blocking, and will not alert you to an entire web site that violates your privacy preferences. It is a publicly available "P3P-enabled search engine. This works by crawling the web and maintaining a P3P cache for every site that ever appears in a search query. The cache is updated every 24 hours so that every policy is guaranteed to be relatively up to date. The service also allows users to quickly determine why a site does not comply with their preferences, as well as allowing them to view a dynamically generated natural language privacy policy based on the P3P data. This is advantageous over simply reading the original natural language privacy policy on a web site because many privacy policies are written in legalese and are extremely convoluted. Additionally, in this case the user does not have to visit the web site to read its privacy policy. Benefits Edit P3P allows browsers to understand their privacy policies in a simplified and organized manner rather than searching throughout the entire website. By setting your own privacy settings on a certain level, P3P will automatically block any cookies that you might not want on your computer. Additionally, the World Wide Web Consortium W3C explains that P3P will allow browsers to transfer user data to services, ultimately promoting an online sharing community. The P3P toolbox site explains how companies have taken individuals data in order to promote new products or services. Furthermore, in recent years companies have taken individuals information and created profiles, which they then market without the individuals consent. Moreover, all this data is misused and we as consumers pay the price and become worrisome of issues such as: Moreover, since there has been an increase of browsers there are more users at risk running into privacy problems. Another concern is that websites are not obligated to use P3P, and neither are Internet users. P3P has been known to undermine public confidence by collecting enormous amounts of information that can be used against its user. Moreover, the EPIC website points out that P3Ps protocol would become burdensome for the browser and not as beneficial or efficient as it was intended to be. The basic idea of privacy protection can be misleading to the visitors on the site. For example, people think that their privacy is actually being protected, but it is not. P3P facilitates data collection from websites. If the actual intention of p3p was to protect visitors to web sites then the information gathering would not be so easy to pass along personal information. Also, people who visit websites where p3p is present are uninformed and misunderstand the level of privacy that p3p provides. There needs to be more effective ways of educating people on the level of privacy and what p3p actually does to protect people. Another main concern is that the data that is collection does not have an expiration date. People who buy something on the internet will have that information saved for an infinite amount of time, whether it will be recorded for a year or ten. This problem has lead people to question where their information is being distributed to and for how long third parties will have access to their

information. A key problem that occurs with the use of P3P is that there is a lack of enforcement. Thus, promises made to users of P3P can go unfulfilled. Currently, there are no actual laws that have been passed by the United States about data protection. Though it would be nice to be able to trust every company that states its use for our information, there is no binding reason that the company must actually adhere to the rules it says it will comply by. Though using P3P technically qualifies as a contract, the lack of federal regulation downplays the need for companies to abide. EPIC, the technologies obviously largest critic, also talks about how the development and implementation of P3P can cause a monopoly of private information. Since it tends to be only major companies who implement P3P on their websites, only these major companies are tending to then gather this information seeing as only their privacy policies can compare to privacy preferences of users. The EPIC website says, "The incredible complexity of P3P, combined with the way that popular browsers are likely to implement the protocol would seem to preclude it as a privacy-protective technology," EPIC continues on to state, "Rather, P3P may actually strengthen the monopoly position over personal information that U. As people become comfortable with P3P, the technology may be limiting the perceived need of related privacy legislation. Michael Kaply from IBM is reported saying the following when the Mozilla Foundation was considering the removal of P3P support from their browser-line [11] Ah the memories. So both our companies wasted immense amounts of time that everyone thought was a crappy proposal to begin with. P3P is among the specifications we are considering for support in the future. There have been some issues with how well P3P will protect privacy, and for that reason we have decided to wait until these are resolved. Alternatives Edit P3P user agents are not the only option available for Internet users that want to ensure their privacy. Two of the main alternatives to P3P include anonymous e-mailers and anonymous proxy servers. Anonymous e-mailers allow Internet users to send safe and secure e-mails by sending and receiving e-mails anonymously [[13]]. The anonymous e-mailer programs protect e-mail through encryption, the process of transforming information to make it unreadable to anyone without the correct key. Encrypting the e-mail allows the user to send or receive e-mails without being tracked or intercepted by others. There are multiple anonymous e-mailers available. Some anonymous e-mailers encrypt only incoming mail, some encrypt only outgoing mail and others encrypt both. Aderes Security is a program that allows users to send anonymous e-mails and to search the web without revealing their identity [14]. CryptoHeaven allows users to send and receive secure e-mails while remaining anonymous [15]. Both require a paid subscription for their services. Every computer is assigned an IP address when it is connected to the Internet. An IP address is essentially a unique ID or address that commercial services and online snoopers can use to track Internet activity and sites users have visited. Anonymous proxy servers can be used to prevent this tracking of personal browsing. There are various tools one can use in order to surf the web anonymously [[17]]. One tool that allows you to search the web anonymously is called The Anonymizer [[18]]. The Anonymizer is software that users can install to their personal computers to hide their IP address while they surf the net. Using this program, users surf like they normally would, but their IP address remains private. The Cloak is another anonymous surfing tool that does not require any downloading any software [19]. In addition to serving as an anonymous proxy server through an encrypted connection, The Cloak allows users to store remote cookies on its site and filter content based on user preferences. The main alternative to P3P may not be these technologies, but instead stronger laws to regulate what kind of information from Internet users can be collected and retained by websites. The act allows individuals to control the type of information that is being collected from them. Various principles are included within the act, such the rule that individual has the right to retrieve the data collected about them at any time under certain conditions. Currently, the United States has no federal law protecting the privacy of personal information shared online. However, there are some sectoral laws at the federal and state level that offer some protection for certain types of information collected about individuals [21]. For example, the Fair Credit Reporting Act FCRA of makes it illegal for consumer reporting agencies to disclose personal information only under three specified circumstances: The act also requires online sites to provide parents with information about their privacy practices and to allow parents to review and correct any personal information

collected about their children. The Future of p3p Edit There are many groups who are working to further the future of p3p to make it easier for people to use. Some of these groups are: The goal of TAMI is to create technical, legal, and policy foundations for transparency and accountability in large-scale aggregation. TAMI hopes to help people manage privacy risks in a world where technology is constantly changing. Policy Aware Web [PAW] is a scalable mechanism for the exchange of rules and proofs for unlimited access control to the Web.

Chapter 3 : Web Privacy with P3P by Lorrie Faith Cranor (, Paperback) | eBay

This text explains the P3P protocol and shows Web site developers how to configure their sites for P3P compliance. Full of examples and case studies, the book delivers practical advice and insider tips.

The options chosen in developing the protocols, grammar, and vocabulary needed for an agreement lead the authors to a number of generalizations regarding the development of technology designed for "social" purposes. In this paper we will explain the goals of P3P; discuss the importance of simplicity, layering, and defaults in the development of social protocols; and examine the sometimes-difficult relationship between technical and policy decisions in this domain. Introduction The relationship between technical choices and the non-technical consequences of those choices is inherently difficult. In this paper we discuss several methods for addressing such "policy" decisions in ways that allow engineers and policy makers to apply the methods of their trade to the questions they are best equipped to solve. Our discussion is motivated by our participation in the Platform for Privacy Preferences Project P3P , a framework for automated decision making about online privacy; however, it is also relevant to a more general set of problems. When the relationship between technical and policy choices is ignored, it may lead to unintended and undesirable consequences, or situations in which technologies can be coerced to effect covert policies. We highlight two examples of these situations: The debate surrounding the Communications Decency Act CDA presents several examples of technologies and proposed technologies that could lead to unintended consequences. For instance one of the proposals for preventing children from accessing harmful materials online would have required the next version of the Internet Protocol to include support for labeling each piece of Internet data with respect to the age of its sender. A note entitled, Enforcing the CDA Improperly May Pervert Internet Architecture, stated that by including such functionality within Internet routers the simplicity, low cost, and radical scalability of the Internet would be jeopardized Reed, No matter what you believe about the issues raised by the Communications Decency Act, I expect that you will agree that the mechanism to carry out such a discussion or implement a resolution is in the agreements and protocols between end users of the network, not in the groups that design and deploy the internal routers and protocols that they implement. I hope you will join in and make suggestions as to the appropriate process to use to discourage the use of inappropriate architectural changes to the fundamental routing architecture of the net to achieve political policy goals. An example of a covert mechanism designed to implement social policy is the decision of mid-twentieth century New York city planner Robert Moses to design his roads and over-passes so as to exclude the foot high public transit buses that carried people -- often poor or of color -- to the parks and beaches he also designed Winner, Not only did he fail to separate the mechanism of transportation from social policy, he did so in such a way that his own biases were substituted in the place of legitimate policy processes. Bob Scheifler, a developer of the X Windows System, did recognize the importance of separating mechanism and policy and is often quoted for his useful maxim of "mechanism not policy. The result was a mechanism that allowed user control over graphical elements and window system. In the online realm, protocols have been developed to solve technical problems such as uniquely addressing computers on a network and preventing network bottlenecks. However, new protocols are being developed that are driven by explicit policy requirements. For example, meta-data -- ways to describe or make statements about other things -- and automated negotiation capabilities are being used as the foundation for applications that mimic the social capabilities we have in the real world: We characterize this breed of protocols -- including P3P -- as social protocols Reagle, In contrast to technical protocols, which typically serve to facilitate machine to machine communications, social protocols often mediate interactions between humans. Many of the lessons learned in the course of P3P can apply to the development of other social protocols such as those designed to facilitate content control, intellectual property rights management, and contract negotiation. In the following sections we present a brief background of the P3P effort from both policy and technical perspectives. We then examine the issues of simplicity versus

sophistication, layering, and defaults to illustrate ways in which non-technical decisions are implicitly incorporated into or promoted by technology; we also present several options and recommendations for designers to consider when attempting to mitigate contentions between technical and policy concerns. Before proceeding, we wish to quickly explain what we mean by "policy" through a simple definition and example. Mechanism is how to technically achieve something, policy is what one wishes to achieve. For example, P3P is a mechanism for expressing privacy practices; European Union data protection concepts are an example of a policy. In general, the separation of mechanism and policy provides for great flexibility and allows non-technical decisions to be made by those most qualified to make them. Parents are particularly concerned about Web sites that collect information from their children CARU, In , several organizations launched efforts to develop "user empowerment" approaches to online privacy Cranor, IPWG is an ad-hoc group coordinated by the Center for Democracy and Technology and is comprised of a broad cross-section of public interest organizations and private industry engaged in commerce and communication on the Internet. Technical Background The Platform for Privacy Preferences is intended to allow sites to express their privacy practices and for users to exercise preferences over those practices. If a relationship is developed, subsequent interactions and any resulting data activities are governed by an agreement between the site and the user. After configuring privacy preferences, individuals should be able to seamlessly browse the Internet; their browsing software user agent negotiates with Web sites and provides access to sites only when a mutually acceptable agreement can be reached. P3P efforts focus on how to exchange privacy statements in a flexible and seamless manner. However, the platform may be used in conjunction with other systems, such as TRUSTe, that provide assurances that privacy statements are accurate. The P3P grammar specifies the types of clauses that comprise P3P statements. For example, the P3P grammar specifies that P3P statements must include, among other things, clauses describing any data that is to be collected and the practices that apply to that data; a vocabulary includes a list of specific data practices that are valid in a practice clause. Multiple rating systems or vocabularies can be developed and used independently. IPWG is in the process of designing one such vocabulary. While PICS provides only for a simple "label" to be used in describing Web content, P3P employs a grammar that allows clauses to be combined to form richer P3P statements. Design Issues for Social Protocols While separating technical decisions from policy decisions is laudable, such separation is not always readily achievable when designing social protocols, as technical and policy decisions often become intertwined. The line between mechanism and policy may be a fuzzy one, and some aspect of the design often falls within the gray area. We explore three themes of social protocol design that are important to P3P: We discuss each with respect to separating mechanism from policy, and when such separation is impossible, we offer potential solutions technologists can use to produce good engineering in the face of contentious policy issues. We address the themes of simplicity, defaults, and layers in separate sections. However, no understanding of one theme can be applied without an understanding of the others. Decisions about how to set defaults and in what layers to address various concerns can impact the overall simplicity of a software tool; indeed layers and defaults can be created specifically to simplify the user experience while providing sophisticated options for the users who want them. Simplicity and Sophistication In early discussions about P3P, its designers considered ideas for elaborate systems that would contain extremely sophisticated and detailed privacy grammars, tools for robust strategic negotiation, automated privacy enforcement ways to automatically penalize "cheaters" , cryptography, certificate schemes, and more. There is relatively little that cannot be seen within scope on first blush. However, designers must often simplify their elaborate ideas in favor of system designs that can be readily implemented and used. With P3P -- as with other projects -- one must strike a balance between sophisticated capabilities and ease of implementation and use. Difficult decisions will always have to be made with respect to defining certain capabilities as out-of-scope, or unattainable. However, a number of techniques also exist whereby one can enable sophisticated capabilities that are realizable, readily comprehensible, and easy to use. Such techniques include breaking a large system into smaller modules modularity , designing a system in layers that have varying levels of accessibility to the

user layering , and building a basic system that allows new features or even entire modules or layers to be plugged-in later extensibility. These techniques also prove useful for separating technical and policy decisions. Descriptive versus Subjective Vocabularies PICS and P3P have both been designed as basic frameworks to support automated decision-making, but neither specifies the details of a decision-making language. PICS allows multiple third parties to provide these details in the form of rating systems; P3P allows these details to be provided in vocabularies. As a result, third parties can design rating systems and vocabularies that are fairly descriptive, or very simple. A sophisticated rating system might have 20 variables that users must set with respect to the type of content they wish to see, while a simple rating might have a single "thumbs up" variable. Each system has its benefits. The sophisticated rating system provides more information, but requires greater user involvement in its configuration. The simple rating system is quite easy to use, but conveys less information. When considering P3P, we are presented with a spectrum of options, ranging from fairly descriptive and sophisticated vocabularies over which users must carefully express their preferences, to simple vocabularies with which users defer the expression of their preferences to others. The degree to which the variables are interrelated is another important factor. A spectrum of rating systems and vocabularies. To draw the line between descriptive and subjective we present the following understanding. Users express preferences over descriptive information in order to reach subjective "opinions" upon which their agents act. Rating systems include both descriptive information and subjective opinion about the appropriateness of content. However, subjective systems can be problematic because users may not know if the bias inherent in the system matches their own. The most common complaint against filtering technologies today is that decisions are opaque, consequently a user may have deferred to biases that would be offensive to the user if known. Also, from descriptive information one can always derive a new set of "subjective" opinions. If you are told about the content of a sites in terms of violence, language, nudity, sex, who paid to produce it, and the intellectual property rights associated with its use, one can make a thumbs up or thumbs down decision. Once opinions replace descriptions, information is lost. Indeed, the choice of which categories to include in a system may be in and of itself a subjective decision Friedman, Thus we prefer to think of systems as relatively descriptive or subjective, rather than absolutely so. Rating systems designed to describe adult content have been criticized for not being able to distinguish artistic nudity from sexual nudity, a distinction that is inherently subjective. The loss of descriptive information is a significant issue when creating systems for international use where laws and culture vary. Descriptive systems fare best, because a cultural group can always operate upon descriptive information, but the biases implicit in a western "thumbs up" may make such information useless to other cultures. The P3P designers have therefore focussed on designing a grammar and vocabulary that allow for the description of how collected information is used rather than subjective statements such as whether information is used in a "responsible" or "appropriate" way. Recommended Settings In the privacy realm both simplicity and sophistication are required. Because people have varying sensitivity towards privacy, we cannot afford to reduce the amount of information expressed to all users to the granularity that is desired by the "lowest common denominator" - those who want the least information. Fortunately, a complex, descriptive vocabulary can be easily translated into simpler, subjective statements. Rather than manually configuring a user agent using the complex vocabulary, an unsophisticated user can select a trusted source from which to obtain a recommended setting in the form of a "canned" configuration file. These are the settings the user agent will use when browsing the Web on behalf of its user. A set of recommended settings may be thought of as a subjective vocabulary and simplified grammar, overlaid on top of a descriptive vocabulary; this is an example of layering, a topic we will address further in the next section. Recommended settings capture valuable subjective information that can simplify the user experience while retaining descriptive information in the vocabulary. Figure 2 shows a sample set of recommended settings with a corresponding complex privacy vocabulary. An organization may develop a single recommended setting that reflects their views about privacy, or, as illustrated in the figure, they may develop several settings to provide a simplified menu of options for users. We hope organizations will develop recommended settings

that users can download and install in their browsers with the click of a mouse. A sample set of recommended settings overlaid on a complex privacy vocabulary. Users can select the setting that corresponds most closely to their privacy preferences rather than individually configuring 35 options. For example, it is common for users of the highly-customizable Unix operating system to copy the configuration files of more experienced users when first starting out on a new system. In the P3P realm, this model has the added policy benefit of making a distinction between the relatively unbiased provision of descriptive information, and those willing to provide recommendations. In such a model, sites would describe their practices in an informative and globally comprehensible vocabulary upon which other entities can make recommendations about how users should act. For example, sites may rate with a descriptive vocabulary such as the one illustrated in Figure 2, but the user need only chose between a small number of recommended settings. Information is not lost, but the user experience is simplified. Defining a Reasonable Grammar We have discussed the use of a descriptive vocabulary over which more subject preferences can be expressed overlaid. In this section we examine the amount of sophistication appropriate for a grammar and the relationship between the grammar and recommended settings.

Chapter 4 : Privacy Policy, Law, and Technology

Deploying P3P on Web Sites. October 2, P3P: Enabling your web site - overview and options. P3P deployment overview. Create a privacy policy Analyze the use of cookies and third-party content on your site Slideshow by zavad.

For Oath products or services that are accessed without signing into an account, this Privacy Policy applies to those products and services starting May 25, If you are creating a new account, the terms below apply starting today. April Our Privacy Pledge Our commitment is to put users first. We strive to be transparent about how we collect and use your information, to keep your information secure and to provide you meaningful choices. Additional privacy practices for certain Services can be found in Details for Specific Products and Services. Your Controls We believe you should have tools to control your information. You can find controls to manage or review your account information, marketing preferences, location data, and search history at Privacy Controls. Some of our Services provide additional controls and privacy practices. Information You Provide to Us. We may collect the information that you provide to us, such as: When you create an account with an Oath Service or brand. When you use our Services to communicate with others or post, upload or store content such as comments, photos, voice inputs, videos, emails, messaging services and attachments. Oath analyzes and stores all communications content, including email content from incoming and outgoing mail. This allows us to deliver, personalize and develop relevant features, content, advertising and Services. When you otherwise use our Services, such as title queries, watch history, page views, search queries, view the content we make available or install any Oath software such as plugins. When you sign up for paid Services, use Services that require your financial information or complete transactions with us or our business partners, we may collect your payment and billing information. We collect information from your devices computers, mobile phones, tablets, etc. This information includes device specific identifiers and information such as IP address , cookie information , mobile device and advertising identifiers, browser version, operating system type and version, mobile network information, device settings, and software data. We may recognize your devices to provide you with personalized experiences and advertising across the devices you use. We collect location information from a variety of sources. Information from Cookies and Other Technologies. These data collection technologies allow us to understand your activity on and off our Services and to collect and store information when you interact with Services we offer to partners. We collect information about you when we receive it from other users, third-parties, and affiliates , such as: When you connect your account to third-party services or sign in using a third-party partner like Facebook or Twitter. From advertisers about your experiences or interactions with their offerings. When we obtain information from third-parties or other companies , such as those that use our Services. This may include your activity on other sites and apps as well as information those third-parties provide to you or us. We may also receive information from Verizon and will honor the choices Verizon customers have made about the uses of this information when we receive and use this data. We also may use the information we have about you for the following purposes: Provide, maintain, improve, and develop relevant features, content, and Services. Analyze your content and other information including emails, instant messages, posts photos, attachments, and other communications. You can review and control certain types of information tied to your Oath account by using Privacy Controls. Fulfill your requests and when authorized by you. Help advertisers and publishers connect to offer relevant advertising in their apps and websites. Contact you with information about your account or with marketing messages, which you can also control. Associate your activity across our Services and your different devices as well as associate any accounts you may use across Oath Services together. We may associate activity and accounts under a single user ID. Carry out or support promotions. Conduct research and support innovation. These analytics and reports may include aggregate or pseudonymized information. Provide location-based Services, advertising, search results, and other content consistent with your location settings. Combine information we have about you with information we obtain from business partners or other companies , such as your activities on other

sites and apps. Detect and defend against fraudulent, abusive, or unlawful activity. We provide you with controls to manage your experience with us. If you opt out, you will continue to see ads, but they may not be as relevant or useful to you. We do not sell, license or share information that individually identifies our customers with companies, organizations or individuals outside of Oath unless one of the following circumstances applies: We will share information with companies, organizations or individuals outside of Oath when we have your consent. Oath affiliates may use the information in a manner consistent with their privacy policies. We may share your information with nonaffiliated companies who are: We provide user information to trusted partners who work on behalf of or with Oath based on our directions and in compliance with appropriate confidentiality measures. For example, we may tell an advertiser how its ads performed or report how many people installed an app after seeing a promotion. When you use third-party apps, websites or other products integrated with our Services, they may collect information about your activities subject to their own terms and privacy policies. Like many companies, we may allow cookie matching with select partners. But, these parties are not authorized to access Oath cookies. For Legal and Other Purposes. We may access, preserve and disclose information to investigate, prevent, or take action in connection with: This may include responding to lawful governmental requests. Learn more about how we evaluate and respond to these requests. If the ownership or control of all or part of Verizon, Oath or a specific Services changes as a result of a merger, acquisition or sale of assets, we may transfer your information to the new owner. Information Security and Data Retention Oath has technical, administrative and physical safeguards in place to help protect against unauthorized access, use or disclosure of customer information we collect or store. To learn more about security, including the steps we have taken and steps you can take, please read Security at Oath. We do not knowingly collect, use, or share information that could reasonably be used to identify children under age 13 without prior parental consent or consistent with applicable law. With parental permission, a child under age 13 might have an Oath Family Account. Data Processing and Transfers When you use or interact with any of our Services, you consent to the data processing, sharing, transferring and uses of your information as outlined in this Privacy Policy. Regardless of the country where you reside, you authorize us to transfer, process, store and use your information in countries other than your own in accordance with this Privacy Policy and to provide you with Services. Some of these countries may not have the same data protection safeguards as the country where you reside. By using our Services, you consent to us transferring information about you to these countries. For more information, please visit our Data Transfer page. This Privacy Policy does not apply to the practices of companies that Oath does not own or control, or to people that Oath does not employ or manage. Changes We may update this Privacy Policy from time to time, so you should check it periodically. If we make changes that are material we will provide you with appropriate notice before such changes take effect.

DOWNLOAD PDF P3P HISTORY ; P3P-ENABLING YOUR WEB SITE : OVERVIEW AND OPTIONS

Chapter 5 : P3P suddenly really unstable in the air. : djiphantom

Introduction to P3P. Week 6 - October 3, 5. P3P: Introduction. Original Idea behind P3P. A framework for automated privacy discussions Web sites disclose their privacy practices in standard machine-readable formats Slideshow by charla.

Where can I get information about how to P3P-enable a web site? For more technical details online, see the P3P Deployment Guide http: For a complete guide to implementing P3P see my book to be published September , Web Privacy with P3P and the accompanying website http: What software can I use to generate P3P policies, compact policies, or policy reference files? You can find a list of P3P policy generators and related tools on the W3C web site at http: There is a similar list at http: What is the easiest way to P3P-enable a web site? P3P enabling a web site is usually a fairly easy process from a technical standpoint. However,it may require web site operators to take a more detailed look at their data practices than they may have done previously,and to coordinate policies and practices across the hosts in their domain. Here is an overview of the steps required to P3P enable a web site. Create a privacy policy. Analyze the use of cookies and third-party content on your site. Determine whether you want to have one P3P policy for your entire site or different P3P policies for different parts of your site -- a single policy for the entire site is easiest. Create a P3P policy or policies for your site. Create a policy reference file for your site. Configure your server for P3P -- for most sites this simply means placing the P3P policy and policy reference files on the server and giving them the appropriate file names; you may also need to configure your servers to send compact policy headers when cookies are set. Test your site to make sure it is properly P3P enabled. The easiest way to P3P enable a site is to create one P3P policy for the entire site and place it on one of your servers. Then place a policy reference file on each host in your domain that references the P3P policy and applies it to all of the content on those servers. Thus you would apply the same policy to all of your content and cookies across every host in your domain. You can create your P3P files using a P3P editor see previous question. This is what most web sites seem to be doing. What do I need to do to prevent IE6 from blocking cookies? The privacy features in IE6 can be used to selectively block cookies based on their P3P compact policies. For detailed information about these features see http: In the default IE6 settings, third-party cookies are blocked when they do not have compact policies or when they have "unsatisfactory" compact policies. To prevent IE6 from blocking cookies on your site you need to make sure that all of the cookies that are being set in a third-party context have compact policies associated with them, and that those compact policies are considered satisfactory see the Microsoft document for the details of what this means. Any host that sets a P3P compact policy must also have a corresponding full P3P policy. Users can change their IE6 settings so that cookies will be blocked under other conditions as well, however, placing satisfactory compact policies on third-party cookies will prevent most IE6 cookie blocking. The simplest thing to do is to arrange your site so that all the content of a particular language is in the same directory. How can I apply different P3P policies to different dynamically generated pages? Some web sites include a lot of dynamically generated content that has URLs that look something like: If we have a form on our site that people can use to sign up to receive a newsletter, what would be the appropriate P3P purpose element? You will also need to specify an "opt-uri" and place a web page at that URI that provides instructions for mailing list removal. How can I figure out what the problem is? This should give you some indication as to where the problem is. Generally the problem is one or more of the following:

Chapter 6 : add a site under a privacy tab of ie through GPO or registry

P3P Enabling your web site overview and options. bring about change throughout history. 68 "Introduction to P3P" is the property of its rightful owner.

P3P is a standard for the declaration of privacy policies in a machine-readable format. The standard allows user agents to make decisions on the part of the user regarding whether to access certain URIs or accept certain cookies based on the policy presented by the Web site. Commercial browsers support P3P, particularly as part of the decision process for accepting or rejecting cookies. Microsoft Internet Explorer 6 has P3P-based cookie filtering enabled by default. Browsers based on Mozilla provide optional P3P cookie filtering. The P3P specification describes a compact policy and a full policy. A compact policy is a subset of a full policy. WebSEAL provides a default compact policy and also provides configuration settings to enable customization of the compact policy. WebSEAL does not provide a full policy. Full policies are specific to the vendor, application, or security environment into which WebSEAL is deployed. Implementation of a full policy is the responsibility of the vendor service provider. WebSEAL includes a configuration setting that can be used to point clients to the location of a full policy. However, an HTTP response can have multiple cookies. Thus, the compact policy specified in the HTTP header applies to all cookies in the response. Since there can be only a single policy, the policy must represent the most strict of the actual policies for the cookies. For WebSEAL, this means, for example, that if session cookies are accepted in a response but failover cookies are not, the worst case P3P policy should be returned for all cookies. The worst case is defined to be the minimum set of conditions that would cause the browser to reject the cookie. WebSEAL returns three types of cookies to the user agent browser: Session cookie Failover cookie e-community cookie There is no need to configure policy for the e-community cookie. The cookie contents are limited to specifying the location of the Web server to which the user authenticated. This cookie contains no information that identifies the user. The session cookie links to session data, and the failover cookie contains enough session information to enable reconstruction of the session. The session cookie is intended only for the origin server, is not retained past the end of the session, and assists in the process of session maintenance. The failover cookie is intended for the failover replicated server, is not retained past the end of the session, and also assists in the process of session maintenance. Thus, session and failover cookies have the same P3P policy. This means that the combined worst case policy for the cookies is the session cookie policy. The complete specification can be accessed at the following URL: This can be used to supply a reference to a full XML policy. The values for purpose except current and recipients except ours have an additional option describing how the cookie data can be used. This defines whether the user is given a choice to opt-in or opt-out. The configuration file entry is: This means that P3P headers from junctioned servers are replaced. When using the default setting, you might find that cookies that the backend server must set are not allowed due to the WebSEAL compact policy. In this case, you should choose one of the following options: Modify the WebSEAL compact policy header to make the policy more permissive, so that backend cookies are allowed. These cookies are used to map URLs across junctions, to ensure connectivity between the browser and the backend server. When the compact policy forbids the addition of the junction cookie, the URL requests from the browser will not successfully resolve to the URLs on the backend server. The header contains a P3P Compact Policy. The policy is a sequence of terms that describe the policy regarding information contained within the cookies in the response. CUR Cookie helps provide the current service. The current service is the access to the protected Web site. OTPi Cookie provides another service, to which the user has opted-in. OUR The Web site itself is the only recipient of the cookie and the information linked to by the cookie NOR Neither the cookie data nor the data to which it links is retained after the user logs out or after the user session expires. UNI The cookie uses a unique identifier that represents the user, by using the session ID and the user name. This step requires determining policy for each of the privacy settings defined by the P3P specification. Web administrators should modify the

default policy as needed to match the site policies for handling of user data in cookies. Web administrators should consult the P3P specification when defining their site policy. Multiple values are allowed for each configuration entry, with the exception of the entries that require a value of yes or no. When a particular configuration entry is not declared, no indicators are added to the compact policy for that entry. Go to the [server] stanza. Decide if P3P headers from junctioned servers will be replaced or preserved. Set the following value: Set this to yes if you want to preserve P3P headers. For more information, see Junction header preservation Go to the [p3p-header] stanza. Specify the access that the user will have to the information in the cookie. Set the value for the following entry:

Chapter 7 : PPT - Introduction to P3P PowerPoint Presentation - ID

Deploying P3P on Web Sites October 2, P3P deployment overview Create a privacy policy Analyze the use of cookies and third-party content on your site Determine whether you want to have one P3P policy for your entire site or different P3P policies for different parts of your site Create a P3P policy (or policies) for your site Create a.

Chapter 8 : How do I view cookies in Internet Explorer 11 using Developer Tools - Stack Overflow

This book explains how the P3P features work in these browsers, and the impact they will have on your web site. Modern software developers, privacy consultants, corporate decision-makers, lawyers, public policy-makers, and many others interested in online privacy issues will make this book an essential addition to their bookshelves.

Chapter 9 : Web privacy with P3P - L. Cranor - Librairie Eyrolles

Frequently Asked Questions About P3P Enabling a Web Site This is a compilation of answers to questions posted on the www-p3p-policy mailing list as well questions about P3P sent directly to me. This file will be updated as additional questions get posted.