

Why is P3P Not a PET?

Ruchika Agrawal

Electronic Privacy Information Center (EPIC)

agrawal@epic.org

Submission to W3C Workshop on the Future of P3P
12-13 November 2002, Dulles, Virginia USA

1 INTRODUCTION

This paper identifies a broad definition and necessary requirements of privacy-enhancing technologies (PETs); provides examples of effective PETs; questions why P3P does not satisfy the definition of PETs; and finally, raises other concerns about P3P.

2 PRIVACY-ENHANCING TECHNOLOGIES

2.1 Broad Definition and Requirements

Privacy-enhancing technologies are protocols, standards, and tools [6] that directly assist in protecting privacy, [3] minimizing the collection of personally identifiable information, and when possible, eliminating the collection of personally identifiable information. [14]

2.2 Examples

Blind Signatures. Blind signatures are an extension of digital signatures. [5] Digital signatures simply ensure authentication, [8] while blind signatures ensure authentication of individuals without identification. [5] One-way functions provide the mathematical foundation for blind signatures, ensuring that the identity of the individual signer cannot be computed in a reasonable amount of time. [18] One application employing blind signatures is the use of "digital cash", which is analogous to the use of hard cash in that it cannot identify the spender while the service provider is assured of the transaction's authenticity. [2] Blind signatures serve as a good example of an effective PET, since blind signatures eliminate the collection of personally identifiable information.

Blind signatures also enable voting that provides authentication without sacrificing privacy. [16]

Anonymous Remailers. An anonymous remailer is a computer program that allows users to anonymously send emails and post to newsgroups. [11] Anonymous remailers are similar to email server software, except that remailers do not log incoming and outgoing traffic information and remailers strip email headers of personally identifiable information. [11] Users can send emails completely anonymously when using a chain of remailers. [11] Anonymous remailers serve as a good example of an effective PET, since anonymous remailers minimize the collection of personally identifiable information, such as a user's name, email address, and IP address that are usually contained in email headers. A number of remailer implementations are currently available.

Web-Surfing Anonymizers. Web-surfing anonymizing tools enable users to surf the web without being tracked, monitored, profiled or exposed to unwarranted cookies, damaging viruses, and unsolicited popup advertisements. [10] Users can visit websites through anonymizing software (as opposed to standard browsers), [10] which for example, can encrypt URLs to circumvent network logging. [1] Web-surfing anonymizers serve as a good example of an effective PET, since Web-surfing

anonymizers minimize the collection of personally identifiable information, such as a user's web-surfing habits. A number of web-surfing anonymizing tools are available today.

2.3 PETs and Fair Information Practices

Fair Information Practices are intended to enable control over personal information. In this respect, techniques that enable enforcement of Fair Information Practices would be considered PETs. An example of Fair Information Practices may be found in the Canadian Standards Association's Model Code for the Protection of Personal Information: [4]

1. **Accountability.** An organization is responsible for personal information under its control and shall designate a person who is accountable for the organization's compliance with the following principles.

2. **Identifying Purposes.** The purposes for which personal information is collected shall be identified but he organization at or before the time the information is collected.

3. **Consent.** The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

4. **Limiting Collection.** The collection of personal information shall be limited to that which is necessary for the purposed identified by the organization. Information shall be collected by fair and lawful means.

5. **Limiting Use, Disclosure, Retention.** Personal information shall not be used or disclosed for purposed other than those for which it was collected, except with the consent of the individual as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

6. **Accuracy.** Personal information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is being used.

7. **Safeguards.** Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

8. **Openness.** An organization shall made readily available to an individual specific information about its policies and practices relating to its handling of personal information.

9. **Individual Access.** Upon request an individual shall be informed of the existence, use, and disclosure of personal information about the individual

and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. Challenging Compliance. An individual shall be able to challenge compliance with the above principles with the person who is accountable within the organization.

3 Is P3P a Privacy-Enhancing Technology?

P3P requires websites to specify their privacy policies in a machine-readable format, for example, XML. [19] Though not required by the P3P protocol, client tools, such as Internet Explorer 6.0 and the AT&T Privacy Bird, may enable users to specify their privacy preferences so that P3P clients may read a website's privacy policy, determine whether the policy satisfies a user's privacy preferences, and warn the user if not. [19] Privacy-enhancing technologies, on the other hand, minimize the collection of identifying data and thus result in far fewer collections of personally identifiable information. [3]

P3P fails as a privacy-enhancing mechanism because P3P does not aim at protecting personal identity, does not aim at minimizing the collection of personally identifiable information, and is on a completely different trajectory than the one prescribed by the definition of PETs. P3P provides no genuine privacy protection: [14] instead of being used to minimize the collection of personally identifiable information, P3P can easily be used to obtain data from consumers by facilitating the collection of personal information through the guise of notice and choice. [13]

The concept of PETs was introduced as early as 1991, [7] preceding P3P. It is not clear why P3P adopts an entirely different set of principles.

4 PROBLEMS WITH IMPLEMENTATION

At best, P3P might be viewed as a Privacy Negotiation Technique (PNT) in that it may enable negotiation among a user and a website. However, even as a PNT, there are still problems.

Why is P3P inaccurate? Or why is P3P not expressive enough to capture intentions? P3P may mark websites as restricted, even when the sites may have very good privacy policies and practices. A recent article in *The New York Times* reported "Indeed, Internet Explorer [as an example of a P3P client implementation] treats some publishers as if they are third parties, even when they are not." [17] The article used iVillage as an example of a website which has not yet put its privacy policy into a P3P-compliant format. Internet Explorer warns iVillage visitors that cookies are being blocked when visitors click on the "My Horoscope" tab.¹ As a result, Vanessa Benfield,

¹ The article reports the technical details: "When users go to iVillage and click on the 'My Horoscope' tab, they are taken to Astrology.com. But at that point, the Internet Explorer sees Astrology.com as the primary

senior vice president of sales for iVillage, users may believe that iVillage's privacy policies are inadequate. Ms. Benfield commented, "The privacy settings for Explorer, while strict, actually aren't as protective as the policy on a lot of sites, including iVillage... The problem comes when you try to turn that policy into a code." [17] Ms. Benfield raises another interesting challenge: how can websites express the intentions of their technologies (e.g. cookies, frames, etc.) via P3P? In particular, distinguishing third-party cookies from first-party cookies, which is the basis for Microsoft's P3P client, does not necessarily capture the intentions behind various cookies.

Why does P3P not ensure that websites conform to their privacy policies? Suppose a user sets his/her privacy protection preferences and a certain site satisfies the criteria (that is, does not get marked as a restricted site). Currently, P3P does not ensure that the website actually conforms to its privacy policies. How can we minimize the resultant false sense of security created for Internet users?

Why is P3P unsuccessful in getting Internet users to play an active role in their privacy protection? Panelists at the Internet Education Foundation sponsored P3P workshop pointed out that while most people acknowledge that their privacy protection is important, most people do not take the time to read privacy policies. [12] Nor do the users pay attention to or tinker with the default settings. [12] Consequently, it is at best uncertain that users will take the time to actively set their privacy preferences or to read the privacy-compliance summaries provided by P3P clients. This challenge of getting users to play an active role in their privacy protection is compounded by the fact that the average person is not technologically savvy.

Why does P3P not address the possibility that Internet users may even decrease their privacy settings so that they can continue with their Internet activities? Some users decrease their privacy settings to gain proper access to particular services.

5 CONCLUDING REMARKS

The concept of PETs was introduced as early as 1991, preceding P3P. It is not clear why the ends achieved by P3P are totally different from those set out in the definition of PETs.

Because P3P does not aim at minimizing the collection of personally identifiable information, P3P is limited in its effectiveness as a privacy-enhancing mechanism. Anonymity tools may be a more useful way to achieve effective privacy protection while still enabling commerce and communication. Another alternative may be to establish a privacy code, such as the Fair Information Practices principles, to which all Internet services would be required to conform. The Canadian Standards Association's Model Code for the Protection of Personal Information is an example of such a scheme. In a report released in May 2000, the United States Federal Trade Commission Chairman pointed out that privacy laws are necessary because consumers are too often asked to

site. iVillage becomes the third party, and cannot track its users with cookies, even though users are still within the iVillage network. There is a further twist: iVillage owns Astrology.com." [17]

concede their privacy for some service or benefit. Consequently, at minimum, privacy technologies should not require nor facilitate consumers conceding privacy in order to participate in commerce. Digital tickets serve as a final example of a better approach to enabling commerce and communication while limiting the collection of personally identifiable information. Our physical world provides ample evidence, including the example of the use of metro cards to authorize a cardholder to ride the metro at any time without the collection or recording of the cardholder's personally identifiable information², thereby demonstrating the effectiveness of this technique.

² Assuming that the metro card was purchased with hard cash.

References

- [1] Anonymizer.com; <http://www.anonymizer.com/> (visited on October 22, 2002).
- [2] Stefan A.Brands; “Untraceable Off-line Cash in Wallets with Observers”; *Advances in Cryptography-CRYPTO '93*; Springer-Verlag; 1994; p.302-318.
- [3] Herbert Burkert; “Privacy-Enhancing Technologies: Typology, Critique, Vision”; *Technology and Privacy: The New Landscape* edited by Philip Agre and Marc Rotenberg; The MIT Press (Cambridge, 1997).
- [4] Canadian Standards Association; Model Code for the Protection of Personal Information (CAN/CSA -Q830-96); 1995;
<http://www.csa.ca/standards/privacy/code/Default.asp?language=English>
- [5] David Chaum, “Achieving Electronic Privacy”; *Scientific American*, August 1992; p. 96-101; <http://ntrg.cs.tcd.ie/mepeirce/Project/Chaum/sciam.html>.
- [6] Roger Clarke; ‘Introducing PITs and PETs: Technologies Affecting Privacy’; February 28, 2001; <http://www.anu.edu.au/people/Roger.Clarke/DV/PITsPETs.html>.
- [7] Roger Clarke; “Roger Clarke's PITs and PETs Resources Site”;
<http://www.anu.edu.au/people/Roger.Clarke/DV/PITsPETsRes.html#Orig> (visited on October 21, 2002).
- [8] Whitfield Diffie and Martin E. Hellman; “New Directions in Ccryptography”; *IEEE Transactionis on Information Theory*; IT-22(6); November 1976.
- [9] Electronic Privacy Information Center and JunkBusters; "Pretty Poor Privacy: An Assessment of P3P and Internet Privacy"; June 2000;
<http://www.epic.org/reports/pretypoorprivacy.html>.
- [10] Simson Garfinkel with Gene Spafford; Web Security, Privacy & Commerce; O'Reilly (Beijing, 2002); Second Edition; p. 262-283.
- [11] Ceki Gulcü and Gene Tsudik; “Mixing E-mail with BABEL”; IBM Research Division, Zurich Research Laboratory; Symposium on Network and Distributed Systems Security; 1996; <http://www.isoc.org/conferences/ndss96/sndss96.htm>.
- [12] Internet Education Foundation (IEF); P3P Workshop; November 16, 2001.s
- [13] Marc Rotenberg, Director of Electronic Privacy Information Center; Hearing on S. 809, The Online Privacy Protection Act of 1999, Before the Subcommittee on Communications Committee on Commerce, Science and Transportation, U.S. Senate; July 27, 1999; www.epic.org/privacy/internet/EPIC_testimony_799.pdf.

[14] Marc Rotenberg, Director of Electronic Privacy Information Center; "Privacy in the Commercial World"; Prepared Witness Testimony, The House Committee on Energy and Commerce, W.J. "Billy" Tauzin, Chairman; March 1, 2001; <http://energycommerce.house.gov/107/hearings/03012001Hearing43/Rotenberg68.htm>.

[15] Marc Rotenberg; "A Way Forward for Data Protection: Privacy Enhancing Technology"; *the PARLIAMENT Magazine*; September 30, 2002.

[16] Bruce Schneier; Applied Cryptography; John Wiley & Sons, Inc. (New York, 1996); p. 126-127.

[17] Bob Tedeschi; "Clash of Internet Privacy Policies"; *The New York Times*; October 14, 2002; <http://www.nytimes.com/2002/10/14/technology/14ECOM.html>.

[18] Peter Wayner; Translucent Databases; Flyzone Press (Baltimore, 2002); p.13, p. 129-131.

[19] World Wide Web Consortium (W3C); *Platform for Privacy Preferences (P3P) Project*; last revised October 23, 2002; <http://www.w3.org/P3P/>.