Position Paper: Incentives for Adoption of Machine-Readable Privacy Notices

Lorrie Faith Cranor
Carnegie Mellon University
November 5, 2010

With increasing recognition that website privacy policies are failing consumers and that data flows are getting increasingly complicated and involve parties unknown to the end user, numerous suggestions[1] are emerging for technical mechanisms that would provide privacy notices in machine-readable form, allowing web browsers, mobile devices, and other tools to act on them automatically and distill them into simple icons for end users.

In many ways, these conversations are reminiscent of those that took place 15 years ago, and which led to the development of the Platform for Privacy Preferences (P3P) standard.[2] P3P was developed with the idea that your web browser should be able to read privacy policies for you without interfering with your web browsing experience. After nearly two years of informal discussions, W3C launched a five-year process that led to the development of the P3P 1.0 specification. P3P 1.0 provides an XML format for website privacy policies, and a protocol for locating and retrieving these policies and associating them with online resources. The P3P 1.0 specification also describes a P3P "compact policy" format for providing a summary of the privacy policy for cookies that can be transferred in an HTTP header. A subsequent P3P 1.1 effort produced a working draft, but the working group was eventually closed due to lack of industry participation. P3P tools have been integrated into the Microsoft Internet Explorer 6, 7, and 8 web browsers, and some versions of Netscape. In addition, a variety of P3P authoring tools[3] have been developed as well as prototype P3P user agents.[4]

Microsoft's decision to base third-party cookie-blocking decisions in Internet Explorer on P3P compact policies led to widespread adoption of P3P among advertising networks and other companies making substantial use of third-party cookies. P3P was adopted by about a third of the most popular websites, but never saw widespread adoption beyond popular

---

[1] Here are just a few recent examples: TRUSTe has stated an intention to support efforts to develop XML privacy policies http://www.truste.com/blog/?p=879 . Mozilla has launched a privacy icons project https://wiki.mozilla.org/Drumbeat/Challenges/Privacy_Icons . The Interactive Advertising Bureau (IAB) CLEAR Ad Notice project plans to integrate XML privacy notices http://www.iab.net/clear .

[2] For a history of P3P see chapter 4 of Lorrie Faith Cranor, *Web Privacy with P3P,* O'Reilly, 2002. For another account of the history and a discussion of related policy issues see: Harry Hochheiser, The Platform for Privacy Preferences as a social protocol, *ACM Transactions on Internet Technology,* 2(4), 2002. For a more recent account see also: Ari Schwartz, Looking Back at P3P: Lessons for the Future, November 2009, http://www.cdt.org/files/pdfs/P3P_Retro_Final_0.pdf

[3] One of the most popular P3P authoring tools is the P3P Policy Editor distributed for free by IBM http://www.alphaworks.ibm.com/tech/p3peditor

[4] I have been involved in the development of an IE browser helper object called Privacy Bird http://privacybird.org and a P3P-enabled search engine called Privacy Finder http://privacyfinder.org . Privacy Finder demonstrates the use of P3P to help users select privacy-protective sites from among search results. It also integrates a privacy "nutrition label" generated automatically from P3P policies http://cups.cs.cmu.edu/privacyLabel/ .

sites and those that use third-party cookies.[5] More recently, our research has found that a large fraction of sites adopting P3P compact policies have misrepresented their privacy practices, most likely in an effort to prevent IE from blocking their cookies. While this would seem to be an area where the US Federal Trade Commission and other regulators could exert their enforcement authority, to date no enforcement actions have been taken based on P3P.[6]

P3P has long been criticized simultaneously for being too complicated, and for not being expressive enough for companies to accurately represent their privacy practices. Indeed, there is a tension between the need to develop a standard that is simple enough to be practically implemented and expressive enough to capture nuances of privacy practices. This tension is exacerbated by the fact that end users and companies often have different ideas about what details of privacy practices are important to represent. Some companies have criticized P3P for exposing the "gory detail" of their privacy practices.[7] Furthermore, P3P compact policies are even less expressive than full P3P policies, and thus present further problems for companies that must rely on them to avoid IE cookie blocking.[8]

P3P 2.0 or a completely new approach to machine-readable privacy policies could be developed. This new approach would certainly benefit from the P3P 1.0 experience and what we've learned over the past 15 years and would hopefully be significantly better. But a technically superior protocol will still not lead to widespread adoption if we do not address the most significant barrier to adoption: lack of incentives. If the new protocol were built into web browsers, search engines, mobile application platforms, and other tools in a meaningful way such that there was an advantage to adopting the protocol, we would see wider adoption. However, in such a scenario, there would also be significant incentives for companies to game the system and misrepresent their policies, so enforcement would be critical. Incentives could also come in the form of regulations that require adoption or provide a safe harbor to companies that adopt the protocol. Before we go too far down the road of developing new machine-readable privacy notices (whether comprehensive website notices like P3P, icon sets, or notices for mobile applications, behavioral advertising, or other anything else), it is important to make sure adequate incentives will be put in place for them to be adopted.

---

[5] L. F. Cranor, S. Egelman, S. Sheng, A. M. McDonald, and A. Chowdhury. P3P deployment on websites. *Electronic Commerce Research and Applications,* 7(3):274{293, 2008. http://lorrie.cranor.org/pubs/p3p-deployment.html

[6] P.G. Leon, L.F. Cranor, A.M. McDonald, and R. McGuire. Token Attempt: The Misrepresentation of Website Privacy Policies through the Misuse of P3P Compact Policy Tokens. WPES 2010. http://www.cylab.cmu.edu/research/techreports/2010/tr_cylab10014.html

[7] Kenneth Lee and Gabriel Speyer, "White Paper: Platform for Privacy Preferences Project (P3P) and Citibank" http://www.w3.org/P3P/Lee_Speyer.html

[8] In 2006 a minor change to the compact policy syntax was proposed in P3P 1.1 http://www.w3.org/TR/P3P11/ to address a common problem and significantly improve expressivity. However, P3P 1.1 was never finalized and this syntax was not adopted in Internet Explorer.