Open Letter to P3P Developers & Replies

Jason Catlett
Junkbusters Corp

http://www.junkbusters.com

Open Letter to:
Lorrie Faith Cranor, AT&T Labs www-p3p-public-comments@w3.org
September 13, 1999

Dear Lorrie and P3P developers

This letter explains why I believe that P3P is unlikely to ever serve the privacy interests of online consumers in the US or elsewhere. On the contrary, it has come to be used by some as an excuse to delay the progress of genuine enforceable privacy rights in the US. I ask you to consider abandoning the project.

My intent in this letter is not to disparage the enormous effort that you and many others have put into the development of the P3P specification. Nor do I wish to impugn your motives in doing so, nor to say that the effort was wasted or unfruitful. I believe technology has an important role to play in protecting privacy, and much remains to be learned on how to best achieve this. (See for example the attached letter to RosettaNet on one opportunity.)

The P3P project has raised some interesting and useful questions, such how to exchange summaries of information practices in "a decentralized and global medium," as you explain in your paper at http://www.w3.org/TR/NOTE-P3P-CACM/ and also http://www.w3.org/People/Reagle/papers/tprc97/tprc-f2m3.html. But there is currently a widespread expectation that P3P will before long solve the privacy problem that makes Jane Doe of Main St hesitate to buy online from a major US cataloger. I don't believe it will; on the contrary I believe that the solution to that problem lies elsewhere and is being delayed by the unrealistic expectations that have accreted around the P3P project. Unjustly, it has been marketers and lobbyists, not the P3P researchers, who have portrayed P3P as the golden pot of consumer privacy just waiting at the end of the technology rainbow. For example, the DMA's comments of July 6, 1998 before the Department of Commerce claimed that technology was playing a leading role in self-regulatory efforts, citing P3P as bringing on a future where "it will be the individual user, rather than industry or government, who will determine the uses of information." The DMA also claimed at that time that P3P "will be soon available." By contrast, the academic papers on P3P have clearly stated its limitations.

But the sad reality is that more than two years — a decade in "Internet time" — has passed since a P3P prototype was demonstrated before the Federal Trade Commission as the great white hope of Internet privacy. The FTC recently sent to Congress a contorted report in which the Commissioners recommended (with dissent) against passing any privacy laws, while encouraging the further development of P3P. Lobbyists continue to describe P3P as the privacy technology of the future, and perhaps they secretly hope that it always will be. Before the P3P developers put even more effort into a project that has little chance of helping privacy, I ask you to review the purpose that P3P is actually serving.

This letter explains why I consider the P3P concept (as promoted by proponents of self-regulation) fundamentally flawed due to the mistaken premises on which they are based. These issues are not terribly new or difficult to understand, but they continue to be ignored. (See for example the EU's opinion at http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp11en.htm or other opinions at http://www.ntia.doc.gov/reports/privacy/selfreg5.htm and http://cyber.law.harvard.edu/people/reagle/privacy-selfreg.html for example.)

To see the absurdity of the current state of American privacy and P3P's part in it, imagine switching the interest concerned from privacy to copyright, a very similar right concerning the restriction of dataflows. Suppose that in response to the music industry's alarm about unauthorized distribution of songs over the Internet, a consumer group proposed a technology called the "Platform for Piracy Promises". Each consumer would configure his own "piracy policy" in his browser, stating the circumstances under which he promises to copy, modify, transmit or broadcast certain different kinds of recordings, such as poetry, country music, and heavy metal containing profane lyrics. A rich language will be developed to express information about the various uses, owners and types of content. When the consumer visits the site of a recording company to download MP3 tracks, his browser would automatically "negotiate" with the company's server to determine whether the consumer's piracy policy "matches" recording company's "preferences" for use of its property. In reality, any sober recording executive presented with this scheme would halt the presentation at the word "preferences" and dismiss the proposal as preposterous. He might point to issues such as enforcement, redress, third parties, complexity, and lack of uniformity. The executive probably wouldn't even bother to point out that the scheme would take years to become prevalent. Clearly what is needed first is a law, and the industry obtained one last year: the Digital Millennium Copyright Act. If asked whether this scheme might help "in a decentralized global medium," the executive would reply that he would want laws and treaties and lot more protection than the say-so of a random foreigner before he releases his precious data. (And indeed this is happening: look at the World Intellectual Property Organization Treaty and the Secure Digital Music Initiative.) He is unlikely to be convinced to wait a few years to see if the Platform for Piracy Promises might somehow work out, and even less likely to hand over his assets in the meantime.

Yet this is the equivalent of what is currently being asked of the American consumer. P3P has little more hope of protecting privacy as the Platform for Piracy Promises has of protecting copyright. As a technologist I'm fascinated by the ideas raised by P3P, but as a privacy advocate I have to take the same hard-nosed attitude as an executive with a responsibility to shareholders. P3P is not going to protect privacy, and the public shouldn't continue to be told it will.

Here are some of the principal flaws in the concept of P3P.

* The concept presumes that privacy is a preference that some technologically advanced minority might be granted an opportunity to avoid having violated on occasions where those people have taken a specific action designated by the companies who wish to exploit personal information. Rather, privacy is a fundamental human right that should be universally expected.

* The concept presumes consumers have an extremely diverse range of "privacy preferences" that should be catered to with a correspondingly wide range of options, like flavors of soft drinks.

Rather, the core of consumers' desires for privacy are simple and easily stated, but unpalatable for marketers: consumers don't want their personal information sold, shared, or reused for secondary purposes. The fact that some are willing to grant specific consent for certain uses doesn't mean that they wish to make an open offer of their privacy. A bewildering range of options tends to to distract consumers and policymakers from the sad fact that what should be standard equipment is hard to find or entirely absent.

* The concept's premise promotes the view that personal information is a secondary currency or commodity to be bartered rather than a necessary detail for performing some part of the transaction, such as delivering the ordered goods by mail. Rather than the fake-privacy doctrine of "notice and choice," which in practice means burdening the consumer with understanding complex details and attempting to opt-out of some of them, real privacy consists of limiting the use of information to what is needed, always with the explicit consent and understanding of the consumer.

* There is a presumption that access should be focused on a company's policy instead of access by individual consumers to information held by the company about them. Rather, a consumer should be able to assume that the company's policy is to treat her data fairly; what she then needs is to be given access to all her specific data so that she can check that it is being correctly handled in practice. She should be able to check that her understanding of what information the company should have about her corresponds with what is actually held, and amend it if not. Granted, P3P does offer a way for a site to say whether it grants access, but stops there. Standards such as the now-moribund Open Profiling Standard can be quickly recognized as marketing mechanisms rather than privacy standards by the fact that the flow of personal information is unidirectional: from the consumer to the company.

* The political environment surrounding the development of P3P promotes the erroneous belief that Internet privacy is something terribly complex and remote from "offline" privacy, and that technology will eventually solve the problem if given time, making legal rights and enforcement mechanisms unnecessary. Rather, the core privacy issues are identical online and offline; online consumers are more aware of the risks, so companies have been forced to give it more attention. Further, no amount of technology can ever make up for the lack of enforceable privacy rights held by the American citizen.

* Perhaps the most implausible premise is the view that a high level of privacy will eventually be achieved if software makers and ecommerce sites agree on a standard that (after an even longer time, as software is upgraded) might be adopted by a sufficiently large percentage of consumers, thus expressing through the market and technology an economic demand for privacy. Believing this process will succeed in protecting privacy is as naive as hoping that environmental protection would be well served by having Exxon and GM draw up standards for emission control, and by the auto industry providing consumers the opportunity to vote on these standards by checking boxes on postcards made available to them at gas stations and automobile showrooms. Rather, technologists should take as their point of departure the strong privacy rights that are being mandated by an increasing number of legislatures, and develop technology that will efficiently and effectively serve people exercising those rights.

* There is an unspoken assumption that as soon as a highly technical language is provided for codifying privacy policies, then marketers will offer good policies in this language. Rather, a simple argument will prove that P3P will never provide the majority with any real privacy protection or even useful guidance. Under the banner of "policy-neutral language," P3P is simply deferring the difficult decision of what the minimum acceptable standard should be. As a thought-experiment, suppose that some time in the 21st century, the P3P language is finalized and the software ready. A decision will have to be made on the defaults, designating the minimum expectation that surfers should have before the browser raises alerts on visiting a substandard site. (For P3P to have any widespread effect, it

would have to be pre-installed in both major browsers, and there would have to be some such default below which an alarm is raised.) This entails a large number of questions to which no consensus answer is ever likely to be found. Should the consumer be alerted if a site's policy:

* says it might sell names if the consumer doesn't separately opt out?

* doesn't provide access to the data held by the company about the person?

* applies its web site privacy policy only to information gathered on the web?

and a hundred other questions like these. It will take at least until the 22nd century for marketers to agree to defaults that are anywhere near the levels that consumers or privacy experts would want. And who would be making the decision on whether this technology and its defaults goes into browsers? Microsoft and AOL/Netscape control more than 90% of the market. Do these companies have a history of choosing privacy-friendly defaults, such as those for cookies? No. Do these companies have a history of placing the privacy of consumers above the commercial interest of themselves and their marketing partners? No. Would they install defaults that alarm prospective purchasers unless stated privacy standards are higher than what they currently offer? Very unlikely. If you disagree, why not issue a public challenge to AOL, Microsoft and other sponsors of P3P and the Direct Marketing Association to propose default settings that they consider would be acceptable. If you receive no satisfactory response, take this as an admission that your project has been used as a pawn in a cynical campaign against privacy. If you receive a sensible response, present it to consumers and consumer advocates and ask whether they consider them acceptable. This exercise is unlikely to succeed in gaining a consensus, and you might as well find out whether it can before going to the mighty effort of finalizing the specification and implementing it.

As a product to protect the privacy of the average American shopper, P3P is doomed to fail, because such an outcome is not in the commercial interests of the organizations who decide whether and how it will be deployed. P3P has become a mirage in the desert of Internet privacy.

I have not considered the extrinsic hurdles faced by P3P, such as the questions of patent infringement and the technical difficulty of implementing the specification. These could probably be overcome given time. But the intrinsic problems above appear impossible to overcome.

The history of P3P is saddening, and so are the lost opportunities where similar technology similarly deployed might have helped with many other problems, such as international issues in consumer protection other than privacy. But here, unlike privacy, business groups are calling for consistent global regulations.

To summarize, I believe that P3P is unlikely ever to be adopted to an effective degree, and will not improve the privacy that Americans have in their own country. If your goal is to protect privacy, please consider devoting your resources to technologies that enhance anonymity or that support access by consumers to the data held about them by organizations. The only reason remaining for companies to keep P3P alive is as an excuse to use in their lobbying against enforceable privacy rights for the American consumer: a Pretext for Privacy Procrastination.

Sincerely

Jason Catlett Junkbusters Corp.

Copy to: Ulf Brühann, DG XV, European Commission Ann Cavoukian, Information and Privacy Commission, Ontario Lorrie Faith Cranor, AT&T Labs Peter Hustinx, Netherlands Data Protection Commission David Medine, Federal Trade Commission Larry Irving, U.S. Dept of Commerce Peter Swire, Office of Management and Budget

REPLIES

Mr. Jason Catlett Founder and CEO Junkbusters Corporation

September 29, 1999

Dear Jason:

Thank you for copying me on your open letter to Lorrie Faith Cranor, head of the development team regarding the Platform for Privacy Preferences (P3P). Given your prominence and history of advocating for the protection of consumer privacy in the electronic world, I reviewed your letter and its arguments closely.

As you know, my office has been a supporter in the development of P3P as a machine-to-machine protocol to allow consumers to respond in an informed way to the stated data use practices of Web sites. We participated in a sub-committee of the P3P project as well as having publicly supported the work of the P3P team in a speech given to the Data Protection Commissioners' Conference in Spain last year. Our involvement was, and continues to be, as a party with no vested interest or business ties. Our goal, like yours, is to advance informational privacy. P3P, once implemented, should, in my view, bring a greater measure of control to the consumer regarding what information he or she decides to share with a Web site and how the information can be used. This will result in more control than consumers currently have, which, at present, is very limited.

Our support of P3P in this context remains unchanged. However, you have raised a number of key points that need to be addressed by the P3P team, especially in the area of communications and marketing. P3P has likely been oversold as the "privacy technology of the future" by lobbyists and third parties outside the P3P team. I agree that the development of privacy standards and regulatory frameworks (whether as legislation, or as an industry developed and policed regulation) have been delayed. However, this cannot be wholly attributed to the expectation, held by some, that P3P will resolve the current privacy issues faced internationally or in the United States. There are social, political and economic forces at work that make this far more complex than laying all the blame on P3P. But that should not stop us from "moving the yard sticks" regarding informational privacy.

We, like you, have not stopped our efforts to promote the importance of rivacy in other areas beyond P3P. My office has been deeply involved in:

* strongly supporting the development and passage of Canadian privacy legislation aimed at the private sector, due out later this year,
* advancing the use of privacy enhancing technologies that give individuals greater control over their personal data.

I agree with you that P3P should not be construed as a promotional tool for self-regulation. P3P is viewed as neutral to the regulatory/standards/legislative environment under which it will operate. As I mentioned, you have identified a number of challenges that the P3P project needs to address. At the top of my list I would put better communication and marketing regarding what P3P will and will not do. This a job for the P3P team and I have committed my office to assist in this area.

Second, I agree with you on the need to explore standards as well as privacy-friendly defaults that could be used by P3P. My understanding is that P3P has already made some headway in that area. P3P has the ability to include third party APPELs (a P3P Preference Exchange Language) that ould act as defaults which a consumer could choose from to identify the actions to take depending on

the type of disclosures made by a Web site. You are right to suggest that standards and defaults are a major challenge, but they are also a necessary step.0

Finally, I agree that the jury is still out as to the level of adoption that P3P will have. Only time will tell. Consumers, as many surveys have shown, place privacy in the on-line world as one of their top concerns.

The arguments you bring forward suggest to me that, rather than simply abandoning P3P, we need to redouble our efforts to address the issues you have raised.

Sincerely yours,

Ann Cavoukian, Ph.D. Commissioner

c.c. Ulf Brhann, DG XV, European Commission Lorrie Faith Cranor, AT&T Labs Peter Hustinx, Netherlands Data Protection Commission David Medine, Federal Trade Commission Larry Irving, U.S. Dept of Commerce Peter Swire, Office of Management and Budget Tara Lemay, Executive Director (President), Electronic Frontier Foundation

---

October 13, 1999

Jason Catlett President JunkBusters Corp.

Dear Jason,

Thank you for your recent letter detailing your concerns with the P3P specification. We hope to dispel the misconceptions that you have of P3P and to clarify the intent and actions of the project. Most of your concerns stem from the assumption that P3P is intended to replace existing or future privacy protections and become the only form of privacy protection worldwide. As is clear from the P3P Guiding Principles, public statements of W3C and the activity on the www-p3p-public-comments@w3.org list, this is not at all the case.

* P3P, by itself, does not protect individual privacy - P3P is a standard that can help users protect their privacy in accordance with existing public policy by promoting openness about data practices and facilitating decisions by individuals.

The W3C is merely a standard setting organization; it does not have the ability to determine public policy. While different members of the W3C may have different reasons for engaging in the process - some of which were mentioned in your letter and some of which were not - nothing in the P3P Specification or the P3P Guiding Principles presumes that P3P is designed to replace public policy or a public policy process. In fact, the Guiding Principles specifically state that P3P "has been designed to be flexible and support a diverse set of user preferences, public policies, service provider polices, and applications." Working group members support a range of policy solutions. Some of the designers openly support the creation of new U.S. privacy laws. Accordingly, P3P is designed to allow for statements about data points, which are in turn directed by law, regulatory procedures, self-regulation or other policies.

Your letter also suggests that P3P may be slowing down the political process in the U.S. However, the Internet is a global, decentralized medium. The standard is not, and should not be designed,

to fit any single country's public policies. We do not believe that the citizens of Sweden, for example, should be denied the ability to map their privacy laws onto the Internet until the U.S. has finished its political process. Therefore, it is essential that P3P implementations and other privacy enhancing technologies move forward.

We also do not believe that P3P is slowing down the political process. In fact, we believe that P3P is helping policy makers understand that the solutions that are created will be more effective and enforceable if compatible with technology. Technologies should support not just anonymity and access, as your statement implies, but all eight OECD principles on the Protection of Privacy and Transborder Flows of Personal Data.

Therefore, we foresee P3P inter-working with other privacy tools to offer a framework that supports public policies and enhances individuals ability to protect their privacy that within that framework. A P3P compliant technology can be designed by implementers to allow individuals to choose to surf only sites provide them with anonymity. But we also realize that not all interactions are best served by anonymity. For example, while there are limited contexts in which health care is sought anonymously, generally it is an identity-based relationship. Accordingly, we set out to provide a framework to support a range of interactions not just anonymous ones.

* Products designed to enhance privacy are being created.

Many products to protect privacy are being created by the private sector with or without the P3P standard (please see the partial list at http://www.w3.org/P3P/implementations). Therefore, it seems that a standard to allow these programs to interact plays a useful role outside of the political process. While there is a question as to whether all of these products will accomplish the goal of protecting privacy, it is obvious that many software companies believe that consumers would like tools that protect privacy. In fact, your company, the JunkBusters=AE Corporation, provides such tools and solutions. We believe that a standard may serve to speed deployment and diversity of products.

* The P3P Process is a deliberative and thoughtful process.

As you suggest in your letter, P3P process has indeed been slow in comparison with many other Internet standards. There are several reasons for the rate at which the P3P process has progressed. Mainly, however, this is because the process has been more inclusive than other standard setting processes. This is the reason that P3P has sought input from the Article 29 Working Group, world wide data protection commissioners, as well as soliciting public comments. These meetings have led to a further discussion of issues with the P3P vocabulary, which will be addressed.

We do agree that the process does need to meet its upcoming deadlines <http://www.w3.org/P3P/schedule.html> in order to maintain credibility. More importantly, it will be essential for companies to follow up with high-quality implementations of P3P so consumers can use the technology rather than the standard simply existing for rhetorical discussion. We also agree that the working group is lacking a comprehensive deployment plan and we plan to address this issue. In the end, we are optimistic that companies will indeed build useful products that meet the final P3P recommendation.

As you can see from the public information available at the P3P site the recommendation is expected to be finalized before the end of January 2000. Therefore, your company still has time to join the W3C and engage in the P3P process in order to help build it into a better standard. Your continued input on the www-p3p-public-comments@w3.org list is of course useful, but your participation in the working group could help to ensure that P3P becomes a successful standard. We hope that you will seriously consider this option.

Sincerely,

Lorrie Cranor, AT&T Ari Schwartz, CDT on behalf of the P3P Specification Working Group

Copy to: Ulf Br=FChann, DG XV, European Commission Ann Cavoukian, Information and Privacy Commission, Ontario Peter Hustinx, Netherlands Data Protection Commission David Medine, Federal Trade Commission Peter Swire, Office of Management and Budget.

Ari Schwartz Policy Analyst Center for Democracy and Technology 1634 Eye Street NW, Suite 1100 Washington, DC 20006 202 637 9800 fax 202 637 0968 ari@cdt.org http://www.cdt.org

Statements from Microsoft and Netscape

In response to a request for a response by P3P developers, Netscape and Microsoft posted the following statements.

Microsoft has been actively involved in the P3P process, has contributed substantially to the P3P syntax, and continues to consider the P3P specification for incorporation in Microsoft products. Microsoft has released enabling technologies for P3P in the past (notably the Profile Assistant in IE4.0), and continues to look for a whole solution that benefits a broad base of consumers before it implements yet another a technology. (1999/10/6)

Netscape has always regarded consumer privacy protection to be of utmost importance to the long-term success of the Internet, and welcomes and supports open, industry-wide, standards-based efforts such as P3P to address the issue. Netscape helped pioneer P3P and continues to contribute to its development. Through Mozilla.org, we have made our source code available to web developers, and this allows anyone to add a P3P implementation to our codebase. (1999/10/8)