P3P – problems, progress, potential

By Alan Pedersen

CAN THE PLATFORM FOR PRIVACY PREFERENCES PROJECT (P3P) become the standard for online privacy? *PL&B International* talks to Laurie Faith Cranor, principal researcher for AT&T Labs and chair of the World Wide Web Consortium's P3P Specification Working Group.

Since its official launch in April 2002, P3P has received a battering from certain quarters of the privacy sector. Consumer campaigners have questioned the protection it promises, analysts point to poor adoption rates, and most companies remain unconvinced. But despite the critics, Laurie Faith Cranor remains upbeat about the future. With support from the World Wide Web Consortium (W3C) and backing from key players in e-commerce, she believes P3P can become a driving force in the battle to place privacy protection on the web.

RELUCTANCE TO ADOPT

The number of businesses building the P3P standard into their websites has been "very modest" according to Ernst & Young. Figures published last October showed that 26 per cent of the 100 most popular US websites had implemented P3P, while only 18 per cent of the top 500 considered it a worthwhile investment. But Cranor argues that a positive spin can be put on the figures when you consider that P3P has been around for less than a year. "Of course I would like to see the take-up go faster, but on the other hand, I'm very encouraged by the progress that we've made so far."

The report card may read "could do better", but getting online giants such as Microsoft, IBM, and AOL on board is a significant achievement. Support from the very top may yet prove to be a powerful persuader for cautious companies still weighing up the pros and cons.

It is the current financial climate, rather than the actual technology itself that has been the most prohibitive factor for businesses, explains Cranor. "Companies are streamlining and downsizing, and anything that they don't see an immediate pay-off for, they are not doing. And that has hurt P3P for the time being."

Although privacy is one of the building blocks for consumer trust, the benefits are difficult to define in terms of dollars or euros. So, when it comes to cutting away the fat from the spending budget, cash-strapped boards are unlikely to go out on a limb for a technology with an unproven track record.

> "I expect that the companies that don't implement P3P are going to stand out as perhaps having something to hide."

Businesses may also question the merits of investing in a technology that relatively few web users have heard of. Cranor admits that consumer awareness is still very low, but says businesses should consider the long-term gains. Forward thinking businesses, she says, have recognised P3P as "something which is going to serve them well in the future, even though it may be hard to put your finger on an immediate tangible benefit."

LEGAL UNCERTAINTIES

Would a website be held legally liable if its P3P policy inaccurately described how it manages customer details? And what would happen if the human-readable privacy statement and the P3P policy are mis-aligned, giving web users two conflicting statements?

Businesses have raised "questions as to the legal standing of a P3P policy," says Cranor, "but the W3C is not a governing body, so we can't decide what the legal standing is." However, she says P3P has received attention from global privacy regulators. In November last year, the W3C held a P3P workshop which included representatives from the European Commission, the New York Attorney General's office, and the Information & Privacy Commissioner for Ontario, Canada. Their initial thoughts, said Cranor, were that P3P policies will be regarded as legally binding. "All of these people agreed that, in their capacity of enforcing their respective laws in their jurisdictions, they would view a P3P policy as equal to a human-readable commitment posted on a website."

Although there is yet to be any formal guidance, Cranor suggests that regulators may, in the future, set out formal positions on the legal implications of P3P. "All the regulators at the workshop are going to do some more thinking about whether there is anything more they can say that will ease company's concerns." [Text on the legal discussions at the P3P workshop can be found at www.w3.org/2002/p3p-ws]

IMPLEMENTATION ISSUES

"For the most part, companies have found that they could implement P3P without a problem," says Cranor. "The technical work involved in implementing

P3P is not that difficult, the bigger issue is getting organisations to fully understand their privacy policies and encode them into a computer-readable format.

"Especially in the US," she continues, "a lot of privacy policies are kind of wishy-washy. P3P forces them to make more concrete statements about what they do and don't do." She says this means organisations will have to look beyond their privacy policies and actually examine how they handle data – what information they collect, how they use it, and so on. "For a company to have a P3P statement that they can stand behind, they need to understand their own practices better than a lot of companies currently do." And while this may mean conducting an audit of the company's practices, Cranor believes it needn't be a painful process. "Some companies felt that forcing themselves to do a self-audit was a positive thing."

COMPACT POLICIES

The key implementation problem for P3P, says Cranor, has been the "compact policy". This is a shortened version of the full P3P policy inserted into the HTTP headers of a web page. It enables web browsers to quickly identify a website's policy on the use of cookies. Microsoft's Internet Explorer 6 browser, for example, reads compact policies and then matches them against the privacy preferences set by the web user. They can then choose to automatically block cookies from websites whose P3P compact policy does not meet their preferences, or those sites that do not have a compact policy.

The current version of the compact policy, explains Cranor, is "not as expressive as the full P3P policy. Companies felt that they were being forced to boil down their policy in a way that over-simplified it. And so their compact policy statements didn't truly reflect their practices.

"Some would like to see the compact policy mechanism just removed altogether," says Cranor, "but there are others who feel it is needed for browser performance issues." During the W3C's P3P workshop in November, it was decided to continue with the compact policy, but make changes to the syntax that will allow it to be a little

more descriptive. "Our goal is to put out a P3P Version 1.1 recommendation that adds as many of these issues as possible within about a year."

Despite limitations with the P3P compact policy, Cranor explains that the full P3P policy is flexible and can, for example, allow organisations to indicate compliance with specific privacy laws. "There is actually a field in the P3P policy that allows you to indicate what laws you are in compliance with," says Cranor. One approach would be to come up with a standard way of referring to, say, the German data protection laws. Then you can have a German P3P user tool that would look for that code in the policy. Another approach is to actually expand the P3P syntax to explain additional things which are mandated under a certain law. The vocabulary is extensive, so anybody can basically add these extensions and you can add them in such a way that P3P user tools which do not understand the extensions can ignore them and still process the policy. But those user tools that do understand the extensions can offer some added benefit to the consumer."

THE CONSUMER ANGLE

The level of consumer take-up may hinge upon how useful and functional the user tools are. The Privacy Bird package – a P3P consumer tool developed by Cranor and AT&T Labs – is a good example of how P3P can work for consumers. Privacy Bird does more than just block cookies. It gives consumers much greater choice when deciding how they wish their information to be used [see www.privacybird.com].

But if P3P is to become a privacy standard, user tools must be able to fuse the functionality of products like Privacy Bird with the mass market penetration of browsers such as Explorer 6. As good a product as it is, the 20,000 or so downloads for Privacy Bird pale into insignificance when compared to the millions of web users who have access to the pre-installed P3P tools on Explorer 6. Cranor explains that Privacy Bird was not designed to be a leading P3P product, but rather a demonstration of the possibilities. "Our hope is that the web

browser companies will get some ideas from the Privacy Bird. Our understanding from speaking with the developers is that they do have plans for further development. They were somewhat rushed in getting their initial implementation of P3P into their browsers, but they do hope to spend some more time working on it in the future."

As the technology matures, says Cranor, more possibilities for using P3P will open up. One possibility is to incorporate P3P into search engines so that web users can identify privacy-compliant sites. Web users could be able to search the Internet for the cheapest retail prices and then automatically check the privacy policy before visiting the site. "Once you have a search engine offering that type of service," says Cranor, "that in itself will be an incentive for websites to be P3P-enabled. We need at least one search engine to step forward and say: 'This is a good idea, we're going to try it.'"

ADDED TRANSPARENCY

For those organisations still wavering, Cranor offers these words of advice. "Customers tend to view companies that are not upfront about their practices with suspicion. P3P makes it very easy to describe what your practices are without the consumer having to read through a long legal document. Going forward, I expect that the companies that don't implement P3P are going to stand out as perhaps having something to hide. Companies that want to be proactive and look good on privacy should be proactive about implementing P3P."

i

Information on P3P can be found at the World Wide Web Consortium (www.w3.org/P3P) website and on Laurie Faith Cranor's website (www.lorrie.cranor.org). Cranor has also published a book entitled "Web Privacy with P3P". For further details see www.p3pbook.com