

Can a “Social” Protocol Help Protect Web Privacy?

Jeffrey R. Williams
Georgetown University Law Center
Information Privacy Seminar
Professor Rotenberg
November 3, 1998
jsquared@erols.com

Fido goes surfing

I call my P3P agent “Fido.” He knows everything about me. When I start up my web browser, Fido asks me which persona I would like to assume. I choose “K” after the Men in Black character, since I want to be totally anonymous for the time being.

First, I go to Yahoo and check the news. Fido is silent because Yahoo could care less about my identity. I notice that some of the advertisements don’t appear. Then I remember that when Fido asked me if I wanted to reveal my email address in order to receive those ads, and I told him no.

To check my grades, I decide to log into StudentAccess system at school. Fido recognizes this site and automatically sends them my “Elroy” persona, which contains only my student ID number and a password.

Then I decide to make a first visit to the Wall Street Journal to read a story recommended by a friend. Fido starts barking that the Journal wants my name, address, and phone number to use to contact me with special deals. He suggests that I create a new persona only for the Journal. Okay? Yes.

Fido asks if he should make up a false identity, or give them my real information. I don’t want any calls, so I tell him to lie. He asks me if I plan to return to the Journal site, or should he just throw the persona away after the session. Save? Sure, call it “Wally.”

Privacy on the web

Many Internet sites are clandestinely collecting personal information while their site is innocently perused. Many are only trying to get an idea about how many people see their site, but others are collecting, analyzing, and selling this information. Several surveys have indicated that users consider this a serious threat to conducting business on the Internet.

There is a wide variety of proposed approaches to protecting user privacy in these situations, including Federal legislation, certification programs, and anonymizing technology.

Most of these internet privacy schemes, including TRUSTe and the Better Business Bureau program, are very simple programs involving logos or certification marks. However, the Platform for Privacy Preferences (P3P) from the World Wide Web Consortium (W3C) is different. [1] Their goal is to change the web into a place where user

privacy preferences and provider privacy practices can be negotiated.

What is the P3P?

The Internet is defined by a set of “protocols” which define the format and sequence of communications over the network. For example, the Internet Protocol (IP) defines a sort of virtual world that only provides the capability to send a single packet to another computer.

The early designers of IP did not conceive all the uses for their protocol. Instead, they created a general purpose platform which would enable a wide variety of higher level applications.

By layering additional protocols on top of IP more complex behavior can be created. Each higher layer adds new capabilities to the IP foundation. For example, the Transmission Control Protocol (TCP) adds additional information to IP packets to ensure that they arrive in the right order. TCP also acknowledges the receipt of information, so senders are guaranteed delivery. And the HyperText Transfer Protocol (HTTP) adds additional capability to TCP. And so on. The lower layers always provide services to upper layers.

P3P adds capability to HTTP. In response to the usual request for information, a P3P enabled server will respond with a “proposal” which requests certain information and indicates how the responses will be protected. The user’s client will respond by accepting or rejecting the proposal [2] This protocol is aptly named a “platform” since it defines a layer designed to facilitate privacy negotiations.

The P3P defines the rules of a bargaining game between automated agents in a web site and a web browser. The designers note that “the most general protocol would

permit an unlimited number of rounds of offers and counter-offers, with offers being either commitments or cheap talk.” [3] However, the P3P negotiation is not this general and involves only a single round.

The P3P designers call this kind of platform a “social” protocol because its goal is to facilitate communication about human preferences, not simply technical network performance. [4] Like IP, P3P is a general purpose platform and has no “built in” policy. Rather, it is a mechanism for allowing a simple dialog about privacy to occur.

The “vocabulary” used by P3P allows negotiation about some of the areas covered in the OECD guidelines, notably data collection directly from the user, limitations on use and disclosure, allowable disclosures, and openness about use and disclosure. The other guidelines are largely unaddressed by P3P, including third party collection, data storage and retention, purpose related controls, data quality, and accountability. [5]

What about privacy?

Examined in isolation, P3P sounds pretty good for user privacy. If users and providers can come to agreements on preferences and practices, everyone should be happy, right?

P3P does provide users the ability to restrict the amount of personal information released to providers. The user are no longer burdened with reading confusing and vague privacy statements on each site. Therefore, users could maintain consistent privacy preferences across a wide range of legal jurisdictions. Potentially, P3P user agents will allow the use of multiple pseudo personae, complete false identities with individualized privacy preferences. [6]

For providers, P3P could build consumer confidence in the Internet, which is good for business. Also, P3P could allow companies to compete based on their privacy protection practices. And P3P will enable providers to quickly get the information they demand.

But...

Especially when viewed in isolation, P3P is no silver bullet. Most importantly, providers might try to use the P3P negotiation process to force users to disclose personal information in exchange for using the site. Users, especially those with particularly restrictive privacy preferences, may have difficulty getting access to any sites on the web. Instead of increasing privacy, P3P would end up being a vehicle for reducing overall privacy. [7]

Further, the process of setting up and managing personae could be difficult. Users may end up relying on the defaults built into their browser. [8] These default settings may not accurately represent the actual privacy preferences of users. And worse, providers may tend to make their sites comply with the default preferences regardless of their actual needs for information. [9]

The European Commission Working Party on the protection of Individuals with regard to the processing of Personal Data raises several additional objections to the P3P vocabulary. Primarily, the concern is that the vocabulary is not expressive enough to implement the policies specified by the EU. Therefore, EU citizens accessing sites outside the EU will not be able to verify that the privacy practices are compliant with the EU law. [10]

Of course, this objection merely acknowledges the fact that the protocol is merely a platform upon which a more expressive negotiation protocol might be built. As such, it

represents a compromise between expressiveness and ease of use.

Another major objection by the Working Party is that nothing in the P3P provides for enforcement, sanctions, or remedies. So many sites may, during P3P negotiation, claim that their protections are significantly stronger than they really are. Although the design team has mentioned the possibility of using P3P to perform automated audits of providers, this is merely another potential use of a general platform.

Finally P3P will actually have to be incorporated in a huge number of web servers, pages, and browsers. Because P3P follows conventions for extending current protocols, this change can be incremental, but there is still a lot of work left to be done. [11]

And what about the law?

Several countries, including the EU, have created legal regimes that are intended to protect user privacy. Because the world is not likely to achieve a “harmonized” set of privacy rules anytime soon, P3P negotiated agreements will very likely provide for a different set of privacy practices than the privacy law of some jurisdictions. [12]

Do the P3P negotiated “contracts” take precedence over the applicable legal rules? Or are the legal rules “mandatory” in that they cannot be contracted around.

At first blush, it seems like users ought to have the last word on how their personal data is to be treated. Different people will have vastly different preferences about privacy. Surely the privacy “right” is a default rule, that people can contract around. Justice Brandeis implied as much by discussing the broad power of consent. If this is the case,

then the legal requirements provide “default” terms that can be overridden by specific contracts.

On the other hand, some rights cannot be negotiated away. Perhaps privacy is such a right and providers must follow the legal rules regardless of what their users desire. In this case, the legal requirements form a “floor” for the agreement and providers must at least meet those requirements.

Centralized or distributed

In any case, legal protections and negotiated privacy contracts are not necessarily competing. In fact, they seem to work together well. Privacy laws ensure that domestic providers provide consistent minimum protections. And negotiated agreements provide users a way to ask for more protection if the domestic law is insufficient for their needs.

Because the web is international and users necessarily have to do business with providers in many different legal jurisdictions, negotiated privacy agreements can help users to establish a consistent set of privacy preferences across these jurisdictions. [13] Both approaches have some enforcement problems, especially in the international context.

Judge Easterbrook cautions against legislating too early, especially where technology is moving fast, recommending that instead we ought to “make rules clear; create property rights where now there are none; and facilitate the formation of bargaining institutions.” [14] As Thomas Jefferson put it, “The way to have good and safe government, is not to trust it all to one, but to divide it among the many...[It is] by placing under every one what his own eye may superintend, that all will be done for the best.” [15]

I believe that Jefferson and Easterbrook would like P3P, because it represents a vision of distributed power where people control their own information and to negotiate about certain practices before sharing that information.

Conclusions

Will P3P negotiation make the web a place where privacy is easier to protect? In the same way that nobody knew what people would build on top of the IP platform, nobody knows. Even its creators cannot know exactly what a P3P enabled web will look like.

I suspect that people will take quickly to the idea of controlling their own arrangements concerning their personal information. But it may be very difficult to manage all the details. And it makes sense to remember that P3P is part of a world with laws and customs. I believe that P3P negotiated agreements will probably play a supporting role to basic legal privacy protections.

Come on, Fido. Let’s get to work.

References

- [1] Resnick, Paul. "Privacy Applications of PICS: the Platform for Internet Content Selection," Proceedings of Federal Trade Commission Public Workshop on Consumer Privacy on the Global Information Infrastructure. 1996. Available at <http://www.si.umich.edu/~presnick/papers/ftc96/testimony.htm>
- [2] Joseph Reagle and Lorrie Faith Cranor, "The Platform for Privacy Preferences P3P Note Draft 31-July-1998." Available at <http://www.w3.org/TR/1998/NOTE-P3P-CACM>
- [3] Lorrie Cranor and Paul Resnick, "Protocols for Automated Negotiations with Buyer Anonymity and Seller Reputations." Available at <http://www.si.umich.edu/~presnick/papers/negotiation>
- [4] Roger Clarke, "Platform for Privacy Preferences: A Critique." Available at <http://www.anu.edu.au/people/Roger.Clarke/DV/P3PCrit.html>
- [5] Lorrie Cranor and Joseph Reagle Jr., "Designing a Social Protocol: Lessons Learned from the Platform for Privacy Preferences" In Jeffrey K. MacKie-Mason and David Waterman, eds., *Telephony, the Internet, and the Media*. Available at <http://www.research.att.com/~lorrie/pubs/dsp>
- [6] Lorrie Cranor, "The Role of Technology In Self-Regulatory Privacy Regimes" available at <http://www.research.att.com/~lorrie/pubs/NTIA.html>
- [7] Marc Rotenberg, "Testimony and Statement for the Record to Subcommittee on Courts and Intellectual Property of House Judiciary Committee." Available at <http://www.house.gov/judiciary/41180.htm>
- [8] Jeremy A. Birchman, "Is P3P the Devil?" Available at <http://cobra.law.miami.edu/~jb0437/paper.html>
- [9] Rick E. Bruner, "P3P: Programming Privacy" in Executive Summary. Available at <http://www.x-summary.com/trends/980630.phtml>
- [10] The European Commission Working Party on the protection of Individuals with regard to the processing of Personal Data, "Platform for Privacy Preferences (P3P) and Open Profiling Standard (OPS)." Available at <http://www.epic.org/privacy/internet/ec-p3p.html>
- [11] Carrie McLaren, "Privacy for Dummies? How Corporations Hide Behind Net Privacy 'Solutions'" Available at <http://www.villagevoice.com/columns/9823/mclaren.shtm>
- [12] "EU Committee Warns P3P, OPS Are Inadequate." Volume 18 Number 13, June 26, 1998. Available at <http://www.privacytimes.com/ss-eu.html>
- [13] Esther Dyson, "Privacy Protection: Time to Think and Act Locally and Globally." Available at <http://www.edventure.com/release1/0498.html>
- [14] Frank H. Easterbrook, "Cyberspace and the Law of the Horse." 1996 U. Chi. Legal F. 207.
- [15] Thomas Jefferson to Joseph Cabell (Feb. 2, 1816), quoted in Post, "Governing Cyberspace," at fn. 26. Available at <http://www.law.cornell.edu/jol/post.html>