

BITS

FINANCIAL SERVICES
R O U N D T A B L E

POSITION PAPER

W3C WORKSHOP ON THE FUTURE OF P3P

NOVEMBER 12 – 13, 2002

INTRODUCTION

This Position Paper is being submitted by BITS, The Technology Group for The Financial Services Roundtable. It represents a synthesis of concerns and recommendations from members of BITS and the Roundtable. Membership in BITS and the Roundtable is reserved for the 100 largest integrated financial services companies in the United States. Included among BITS and Roundtable members with an active interest in P3P are Bank of America, BANK ONE, Citigroup, Fidelity Investments, FleetBoston, JP Morgan Chase, Mellon Financial, Northern Trust, Sun Trust, Wachovia, and Wells Fargo & Company.

We appreciated the opportunity to submit comments on the September 24, 2001 Working Draft of the P3P 1.0 specification and the subsequent interactions representative BITS members and staff have had concerning issues we have raised. These comments are intended to build on our previous discussions and to reinforce our interest in working cooperatively with the W3C on both near-term and long-term improvements to the P3P specification.

LEGAL, REGULATORY AND POLICY ISSUES: CONCERNS AND RECOMMENDATIONS

Legal Standing

We remain concerned about potential legal issues surrounding interpretation of P3P. To that end, we continue to think it appropriate and helpful for W3C to state explicitly that P3P is neither a legal nor an audit standard and should not be treated as such. Our members remain convinced that it is the human readable Privacy Policies that are the most comprehensive and complete, and should therefore be those considered to have legal standing. Indeed, the P3P vocabulary itself is not yet capable of precisely replicating human readable policies.

Under current circumstances, BITS members agree with the statement made in the Citigroup position paper of September 2002 that “the dominance of the human readable notice is the only way to provide legal certainty to corporations, government agencies, or others who implement P3P on their Internet sites.”

One example of the limits of the current vocabulary is that financial institutions have used the word “may” in their privacy policies to indicate instances where action using information may or may not be taken. In many instances the circumstances under which a decision is made to use information are complex. Spelling out those circumstances may be undesirable from several perspectives—adding language to already overly complex privacy statements, sharing competitive processes with others, etc. Yet, in the current P3P language, “may” means “will.” This results in an inaccurate expression of the human readable policy.

We understand and agree with the goal that there should be no inconsistencies between the human readable and P3P implementations, however, with that as an assumption, it is the human readable that should dominate and have precedence. The fundamental problem, as we see it, is that P3P as currently written is not rich enough to cover all the points addressed in the human readable Privacy Policies. Ideally, P3P should be capable of tracking exactly to human readable policy. Since it cannot at present, it is all the more important that the human readable policy be viewed as that with legal precedence.

We propose that these limitations of vocabulary be a topic for discussion at the November workshop so that they may be addressed and resolved before the release of the next version of P3P.

It would be helpful for the W3C to state explicitly that P3P statements and compact policies are not meant to be legally binding documents. A clear statement to this effect would encourage quicker and more widespread implementation of P3P. It would also further adoption were there to be standard language issued by W3C to clarify the legal context which could be included in institutions' human readable policies. The language would state something to the effect, “Every effort has been made to comply with the P3P specification; however, given the current limits of the vocabulary, the human readable policy is the most comprehensive, accurate and legally binding.” Regulated sites would be well served if this concept were made part of the P3P specification itself. The specification could indicate that in some circumstances, to more completely reflect the scope and substance of an institution's privacy policy, users may be directed to the institution's plain language policy. We propose that this topic be discussed at the November workshop, and that standard language for incorporation into the next version of P3P be considered and crafted.

A related concern is that there are potential conflicts between how a P3P-equipped browser or tool implementation characterizes site behavior and a company's own plain language privacy policy. This can lead to charges of bad faith and contribute to customer confusion. In the experience of BITS members, two different implementations, reading the same XML statement, could yield two different translations. Such inconsistencies are again confusing to customers and for those attempting to implement the specification at Web sites. We encourage a discussion of what it means to be P3P-compliant, and serious consideration of steps that could be taken to reduce the ambiguity and increase the specificity with which such implementations occur.

One example can appear through the ways in which IE6.0 and AT&T's *Privacy Bird* interpret a site's Privacy Policy. A customer will get different kinds of warnings, depending on the implementation. At the "medium" or "medium high" setting, IE 6.0 may not signal a privacy warning to a user; however, on the same Web site, *Privacy Bird* at the "medium" setting will issue an alert. (The "bird" turns red.) This is confusing. While we think that ambiguity surrounding details of implementation was initially a design decision on the part of W3C, hindsight may suggest that it is time to revisit the decision. The lack of consistency, insufficient clarity, and lack of enforcement of what it means to be compliant are resulting in confusion and lack of coherence in the implementation process.

Implementation Concerns and Legal Complexities Associated with GLBA

With the passage of the Gramm-Leach-Bliley Act (GLBA), additional requirements are in place which must be addressed and implemented by financial institutions. Already highly regulated, financial institutions have invested significant resources in meeting and at times exceeding the requirements of GLBA. A problem has arisen in that there is a mis-match between some GLBA requirements and the *de facto* minimum threshold standards that are set by some P3P implementations. Institutions that have no difficulty in conforming to the requirements of GLBA find inconsistencies and unintended consequences when trying to implement P3P. As a result, with the legal and regulatory oversight tied to GLBA, many financial institutions are making a choice not to implement P3P until the problems are addressed through the W3C and by pervasive User Agents.

While some of these issues may seem beyond the concern of the W3C, it is important that they be fully understood. Until they are resolved, they serve as impediments to the adoption of P3P.

For example, Microsoft's Internet Explorer 6.0, presently the most widely used User Agent, is quickly becoming a *de facto* standard, with over 40% of users browsing financial institution Web sites using IE 6.0. Some characteristics of Microsoft's implementation are creating significant problems for financial institution Web sites. The most significant problems occur in financial portals that aggregate numerous third parties under a single umbrella. In order for these portals to work seamlessly, all the third parties must be willing to post P3P policies or enact P3P-evasive IE-6/P3P behaviors. Since those aspects of P3P that flag problems within the IE 6 implementation do not align with the requirements of GLBA, financial institutions are reluctant to post P3P-compliant policies.

To address industry-specific issues such as these, BITS recommends that the W3C provide for a special U.S. financial institution category within the P3P specification. Qualification for designation within this category would be based on compliance with GLBA as well as other industry rules that address information-use issues, such as the Fair Credit Reporting Act (FCRA). The P3P specification would state that the Web sites of financial institutions in this category are GLBA/FCRA compliant. Further, we recommend that the P3P specification state that User Agents must accept this special financial institution category, enabling implementation without flags that suggest these financial institutions are out of compliance.

Further, we recommend that the P3P specification indicate with precision what English language User Agents should display to users. At present, variations in the language of various User Agents are serving as fodder for attorneys and privacy officers, leading to their advice that financial institutions not post a P3P compliant policy and properly choosing consistency with the law.

Even better, although it could be in addition to the recommendation above, we suggest that BITS work with the W3C to develop a P3P policy—including any new P3P terms that would reflect compliance with GLBA—that a U.S. bank could use and which would reflect privacy policies unique to banks that do not conflict with GLBA requirements.

Under these circumstances, given implementation of these recommendations, it would then be possible for financial institutions to post a P3P policy without the current degree of cautions and concerns from legal and privacy staffs of our member institutions. Implementation of these recommendations, plus the recommendation above concerning Legal Standing, would provide significant encouragement and momentum for financial institutions to take the necessary steps to implement P3P.

EVOLUTION OF P3P: COOPERATION AND COLLABORATION

We appreciate and commend the statements from the W3C that reinforce the perception of P3P as an evolving tool. For example, statements in the Background for the November 12 – 13 W3C Workshop on the Future of P3P are illustrative—“as Web sites adopt P3P, limitations have been discovered and new features are being suggested for possible inclusion in P3P 1.x or P3P2.” Such statements are directionally correct, supportive of an evolutionary view, and serve as encouragement to individuals, organizations, and communities of users to participate in the process to continually improve this tool and its related applications. Members of BITS and the Roundtable stand ready to participate in this ongoing process.

FOR ADDITIONAL INFORMATION:

Contact Cheryl Charles, Ph.D., Senior Director, BITS, The Financial Services Roundtable, 202-289-4322; Cheryl@fsround.org.