EUROPEAN COMMISSION
DIRECTORATE GENERAL XV
Internal Market and Financial Services
Free movement of information, company law and financial information
Free movement of information and data protection, including international aspects

XV D/5032/98
WP 11

Working Party on the Protection of Individuals with regard to the processing of Personal Data

OPINION 1/98

Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS)

Adopted by the Working Party on 16 June 1998

Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS)

Opinion of the Working Party

The Platform for Privacy Preferences Project (P3P) conceives of privacy and data protection as something to be agreed between the Internet user, whose data are collected, and the website that collects the data. The philosophy is based on the idea that the user consents to the collection of his personal data by a site (the Open Profiling Standard is intended to provide for secure transmission of a standard profile of personal data), provided that the site's declared privacy practices, such as the purposes for which data are collected and whether or not data are used for secondary purposes or passed on to third parties, satisfy the user's requirements. The World Wide Web Consortium has sought to develop a single vocabulary through which a user's preferences and the site's practices are articulated. The possibility of adapting this vocabulary to the needs and regulatory context of specific geographic regions is not envisaged. Surprisingly, given the intention that P3P be applicable worldwide, the vocabulary has not been developed with reference to the highest known standards of data protection and privacy, but has instead sought to formalise lower common standards. These policy decisions mean that the implementation of P3P and OPS within the European Union is likely to raise a number of specific problems, which are discussed below. If P3P and OPS are to have a positive impact on privacy protection in the on-line environment, it is essential that these issues are addressed.

- A technical platform for privacy protection will not in itself be sufficient to protect privacy on the Web. It must be applied within the context of a framework of enforceable data protection rules, which provide a minimum and non-negotiable level of privacy protection for all individuals. Use of P3P and OPS in the absence of such a framework risks shifting the onus primarily onto the individual user to protect himself, a development which would undermine the internationally established principle that it is the 'data controller' who is responsible for complying with data protection principles (OECD Guidelines 1980, Council of Europe Convention No108 1981, UN Guidelines 1990, EU Directives 95/46/EC and 97/66/EC). Such an inversion of responsibility also assumes a level of knowledge about the risks posed by data processing to individual privacy that cannot realistically be expected of most citizens.

- There is a risk that P3P, once implemented in the next generation of browsing software, could mislead EU-based operators into believing that they can be discharged of certain of their legal obligations (e.g. granting individual users a right of access to their data) if the individual user consents to this as part of the on-line negotiation. In fact those businesses, organisations and individuals established within the EU and providing services over the Internet will in any case be required to follow the rules established in the data protection directive 95/46/EC (as implemented in national law) as regards any personal data that they collect and process. P3P might thus cause confusion not only among operators as to their obligations, but also among Internet users as to the nature of their data protection rights. Browsing software that is sold or distributed within the EU must therefore

be designed and configured so as to ensure that on-line agreements which are in contradiction with prevailing data protection laws are not possible.

- For users based in the EU entering into contact with websites established in non-EU countries the prime concern is that the organisation to whom they are providing personal data might not be subject to the EU directive or any adequate set of effectively implemented data protection rules [1]. Crucial to the decision of whether or not to provide data to such sites will be to know not only the approximate content of any applicable rules, but also whether there are any sanctions for non-compliance and, most importantly of all, a simple and effective means of obtaining a remedy if the rules are broken. An on-line platform for privacy preferences should in theory be capable of providing such information to users. However, the P3P vocabulary as presently constituted does not require or even allow for the provision of information about sanctions or remedies to users. For P3P to be a useful tool in the obtaining of informed on-line consent for transfers of personal data from EU users (as required by Article 26(1)(a) of the directive), it is therefore necessary to revisit the standard vocabulary.

- Given that most Internet users are unlikely to alter any pre-configured settings on their browser, the 'default' position regarding a user's privacy preferences will have a major impact on the overall level of on-line privacy protection. P3P and OPS must be implemented into browser technology with default positions which reflect the user's interest to enjoy a high level of privacy protection (including the ability to browse websites anonymously) without finding himself blocked or inconvenienced in his attempts to gain access to sites. Where an operator requests, as a condition for access to his site, the provision of a profile of identifiable data, the user should be asked each time for his consent for the provision of this information to the particular site in question. Where a site does not require such information, access could be seamless. The major browsing software manufacturers have a responsibility to implement P3P and OPS in a manner that enhances rather than reduces levels of privacy protection.

Given the importance of the implementation process of P3P and OPS, and the separate issues currently under consideration by the Working Party in relation to the functionality of web protocols (HTTP), the Working Party encourages the development of Internet software consistent with the data protection rules applicable in the European Union and considers that it would be appropriate to develop mechanisms to verify the conformity of Internet software in this regard.

Done at Brussels, 16 June 1998

For the Working Party

The Chairman

P.J. HUSTINX

[1] This is without prejudice to a more detailed examination of Article 4 of directive 95/46/EC, which could be construed as rendering the directive applicable to third country websites collecting data from EU-based users.