Platform for privacy preference (P3P)

Dinant, Jean-Marc

Published in:
User Identification and Privacy Protection. Application in Public Administration and Electronic Commerce

Publication date:
1999

Document Version
Publisher's PDF, also known as Version of record

Link to publication

Citation for pulished version (HARVARD):
Dinant, J-M 1999, Platform for privacy preference (P3P): Finally the convergence between law and technology. How far can P3P guarantee the respect of the European Data Protection directive requirements. in *User Identification and Privacy Protection. Application in Public Administration and Electronic Commerce.* DSV, Stockholm, pp. 43-57.

Platform for Privacy Preferences (P3P) :

How Far can P3P Guarantee the Respect of the Data Protection Directive Requirements?

By Jean-Marc Dinant (**jmdinant@fundp.ac.be**).

The opinion expressed below are those of the author.

This paper has already be presented at IFIP Conference on User Identification & Privacy Protection, Stockholm, 14 June 1999

Key words: Privacy, Data Protection, Privacy Enhancing Technologies, Internet, Invisible Processing, P3P, PICS, W3C, Law and Technology Convergence, Cookies, Processor Serial Number, Global Unique Identifier, HTTP

Abstract: Code of conduct, self-regulation by the industry, enforcement by law, quality label and **P**rivacy **E**nhancing **T**echnologies are some of the solutions available today to promote or ensure privacy on the Web. Among the PETs, P3P seem today be the major technical response from the industry to solve privacy problems on the Internet. It still remain difficult to estimate the accuracy of the P3P approach before the implementation and namely before knowing the defaults setting and the kind of information given to the average netizen.

From the legal point of view, the utilisation of P3P will not exempt data controllers from other duties like providing an access, -and in some cases,- an opposition right, securing the data, collecting not excessive data regarding the declared purpose, etc. In the best case, P3P can just solve the problem of fair information while collecting the data.

From the technical viewpoint, P3P will not solve existing privacy problems created by the conjunction of browser chattering, invisible automatic hyperlinks to third parties and cookies, by the Intel Processor Serial Number or by the Global Unique IDentifier created by Microsoft.

Depending on implementation, P3P can be a good solution to improve privacy on the Net, athought it will not be, at the present stage, the panacea to solve privacy misuses on the Internet.

1 The privacy killing side of the Internet Technology

Before examining the adequacy of a technical disposal to ensure and/or to promote the privacy on the Internet, it appears worthwhile, - in spite of the fact that such approach remains too unusual in the scientific community -, to analyse the privacy killing side of the Internet technology. As a matter of example, we will focus this analysis not on the entire Internet but on the HTTP protocol as it has been widely implemented on common browsers. This field of investigation is very narrow because it excludes

- the privacy killing hardware and namely the problem of the Intel Processor Serial Number[1] or the transmission of the Ethernet card identifier;
- privacy killing piece of software like the Microsoft Personal Identification Number stored in each Word or Excel document;
- others Internet protocols widely implemented in common browsers like POP3, SMTP, FTP or NNTP and…TCP/IP.
-

[1] A description of the Intel PSN controversy can be found on http://www.bigbrotherinside.com. Intel announced on January 1999 that he was planning to include a unique Processor Serial Number (PSN) in every one of its new Pentium III chips (earlier implementations in PII for laptops have been reported). According to Intel, the PSN will be used to identify users in electronic commerce and other net-based applications. Many privacy advocates organisations has protested and asked the FTC to oblige Intel to suppress the accessibility of the PSN via the Internet.

But, at the same time, this arbitrary limitation permits a deep investigation of what happens on the net while surfing. This analysis should be done for every Internet protocol. This paper focuses on HTTP because it is the most widely used protocol and because it can appear at first glance as being inoffensive from a privacy point of view.

Besides privacy harmful content lying in HTML code and embedded in JavaScript[2] or Java applets[3], the HTTP protocol in himself provides at least three characteristics which, combined each with others, forms a privacy killing cocktail widely and daily used by cybermarketing companies.

1.1 The browser's chattering

Every surfer know that typing http://www.website.org/index.htm means something like "show me the page named "index.htm" on the server www.website.org by using the HTTP protocol. One can conclude that no more than the TCP/IP address of the surfer and the file he wants to see are transmitted to the Web site. This is not correct. Here below are listed some of the data systematically transmitted in the HTTP header while doing the HTTP request.

TABLE I :AUTOMATIC BROWSER CHATTERING WHILE DOING HTTP REQUEST

HTTP Var.	***Opera 3.50***	***Netscape 4.0 Fr***	***Explorer 4.0 UK***
GET	GET /index.html HTTP/1.0	GET /index.html HTTP/1.0	GET /index.html HTTP/1.0
User-Agent:	Mozilla/4.0(compatible; Opera/3.0; Windows 95) 3.50	Mozilla/4.04 [fr] (Win95; I ;Nav)	Mozilla/4.0 (compatible; MSIE 4.01; Windows 95)
Accept :	image/gif, image/x-xbitmap, image/jpeg, */*	image/gif, image/x-xbitmap, image/jpeg	image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel, application/msword, application/vnd.ms-powerpoint, */*
Referer :		Where.were.you/doc.htm	Where.were.you/doc.htm
Language :		fr	fr-be

The technical definition of those fields can be found in the RFC 1945[4] for HTTP 1.0 or in the RFC 2068[5] for HTTP 1.1. We can notice

□ The first line is the only which remains indispensable

□ In the Accept: line, every browser is telling that the netizen is using Windows 95 (why?). Netscape adds that the browser version is a French one. Every browser give his own name, version and sub-version identification.

□ While describing the accepted formats, Microsoft tells every site that the netizen's computer has Power-point, Excel, and Word installed on it.

□ Opera doesn't disclose the referring page.

□ Opera doesn't reveal the language spoken. Netscape reveals that the netizen is French speaking. Micro-soft reveal that the netizen is Belgian, French speaking.

[2] See namely the Cuartango Hole which permits to a web site to read any file on the netizen PC while accessing to him : http://www.nwnetworks.com/cuartango.htm

[3] The latest version of Mcafee permits the disabling of such malicious applets or Active-X controls.

[4] http://www.w3.org/Protocols/rfc1945/rfc1945

[5] http://www.w3.org/Protocols/rfc2068/rfc2068

1.2 Invisible hyperlinks[6]

Hyperlinks are the added value of Internet. It permits browsing from one continent to the other simply by a mouse click. What is hidden to the eyes of the common user is that classical browsing software enables to include HTTP requests to download images to be included in the HTML page code. Those images have not to be located on the same server as the one who has received the original call for a particular Web page. In this case, the HTTP_REFERER variable contains the referring page reference, i.e. the main page in which the images will be located. Within others words : if a Web site includes in its Web page in HTML an invisible link to an image located on the Web site of a cybermarketing company, this last one will know the referring page *before* sending the advertising banner. While doing a research on a search engine the name of the Web page includes the keywords typed.

1.3 Cookies

The cookies issues have already been widely discussed[7]. The SET-COOKIE is taking place in the HTTP response header[8], namely in invisible hyperlinks. If a duration is mentioned[9], the cookie will be stored on the netizen's hard disk and sent back to the Web site originating the cookie (or Web sites from the same sub domain). This sending back will take the form of a COOKIE field taking place in the browser chattering described above. When put together with browser chattering and invisible hyperlinks, it means that, by default[10], a cybermarketing company knows all the keywords typed by a particular netizen[11] on the search engine on which he is advertising, the computer, operating system, browser brand of the netizen, the TCP/IP address he has using and the time and duration of the HTTP sessions. Those raw data permit to infer some new data like[12]

1. The country where the netizen live
2. The Internet domain to which he belongs
3. Sector of activity of the company employing the netizen
4. Turnover and size of the employing company
5. Function and position of the surfer within this company

[6] Invisible hyperlink seems us a better wording than the wording used by David Kristol in the so-called cookies II specification (http://www.w3.org/Protocols/rfc2109/rfc2109). D. Kristol spoke about unverifiable hyperlinks. In fact, those hidden hyperlinks are verifiable. But, due to the fact that they are not visible and automatic, they remains widely unverified.

[7] Viktor Mayer-Schönberger*, " The Internet and Privacy Legislation: Cookies for a Treat?"*, http://www.wvjolt.wvu.edu/wvjolt/current/issue1/articles/mayer/mayer.htm; Stephen H. Wildstrom, "*Privacy and the Cookie Monster*", Business Week, December 1996.

[8] Technically speaking, it is also possible to implement cookies in JavaScript or in the <META-HTTP EQUIV> fields located in the HTML code. For more information see http://www.junkbusters.com/ht/en/ijbfaq.html#cookies

[9] Cookies with no duration specified are called "session cookies" and disappear when the browser is unloaded or when the socket close.

[10] Recent browsers provide the ability to block unwanted cookies. See point 4.1 below.

[11] More precisely, those data are linked to a particular personal computer that can be used by many people. From a legal point of view, those data has to be considered as personal data, just as it is already the case with plate and phone numbers which are considered unanimously as being personal data in the sense of art. 2 a) of the European directive 95/46.

[12] Serge Gauthronet, "On-line services and data protection and the protection of privacy" European Commission, 1998, p.31 and 92 available at http://europa.eu.int/comm/dg15/en/media/dataprot/studies/servint.htm

6. Internet Access Provider
7. Typology of Web sites currently visited.

The cookie permits a permanent and unique identifier systematically sent with every request of information while the TCP/IP address remains a relatively weak identifier because it can be hidden by proxies and due to its dynamic characteristic for netizens accessing to Internet by modem. Such invisible profiling has been already done by many US cybermarketing companies and many tens of millions of European netizens are probably profiled in the database of Double Click in New York[13].

1.4 The liability of the Internet Industry

Such a profiling is not "per se" linked to the HTTP protocol, as he has been defined by the W3C[14]. Even more, the HTTP 1.1 protocol definition has explicitly draw the attention of the industry to possible privacy attempts while doing the implementation of the HTTP protocol[15] :

- "*Having the user agent describe its capabilities in every request can be both very inefficient (given that only a small percentage of responses have multiple representations) and a potential violation of the user's privacy*" [page 68 below]
- " *It may be contrary to the privacy expectations of the user to send an Accept-Language header with the complete linguistic preferences of the user in every request*" [page 98]
- " *The client SHOULD not send the From header*[16] *field without the user's approval, as it may conflict with the user's privacy interests or their site's security policy. It is strongly recommended that the user be able to disable, enable, and modify the value of this field at any time prior to a request.*" [page 118]
- "*HTTP clients are often privy to large amounts of personal information (e.g. the user's name, location, mail address, passwords, encryption keys, etc.), and SHOULD be very careful to prevent unintentional leakage of this information via the HTTP protocol to other sources. We very strongly recommend that a convenient interface be provided for the user to control dissemination of such information, and that designers and implementers be particularly careful in this area. History shows that errors in this area are often both serious security and/or privacy problems, and often generate highly adverse publicity for the implementer's company.*" [page 143]
- etc : The word "privacy appears 18 times in the RFC 2068.

By using a specific browser or a technical solution such as Mcafee antiviral shield or a proxy server like the one distributed by Junkbunster, it is possible to surf without invisible hyperlink and/or with less chattering in the HTTP protocol, but, strangely, at the information age, such solution remains widely unused. This last point demonstrates that the common surfing programs are privacy killing, by the implementation choices done by the Internet industry and that the Internet is not privacy killing in itself.

[13] For Double click only, about 26 millions netizens in March 1997 (Gauthronet, op. cit., p. 86) and more then thousand millions of cybermarketing banners downloaded each month outside US (ibid., p. 96)

[14] The World Wide Web Consortium is a non profit organisation hosted by Inria (France), MIT (USA) and the University of Keio (Japan). The members of this consortium are notably Microsoft, AOL, Netscape, …and Center for Democracy and Technology (http://www.w3.org/Consortium/Member/List). This consortium produce non mandatory but de facto normalisation intended to guarantee the interoperability of computers on the Internet.

[15] http://www.w3.org/Protocols/rfc2068/rfc2068 . The page numbering indicated between brackets refer to the numeration of W3C.

[16] Note of the author : From header field is used for naming the referring page

1.5 Specification for a privacy compliant cookie.

The privacy killing side of the cookie lies in to the way in which it has been used. The principle of “notice and choice” can easily be applied to a cookie. Under article 10 of the European Directive 95/46, it means that before sending a SET COOKIE header, a Web site has to inform the consumer by communicating

a) his identity,
b) what information will be stored in the cookie
c) the purpose for which he intends to use this information.
d) the recipients of the collected information
e) which data are mandatory and what happen if not given
f) the existence of an access and rectification right
g) the existence of an opposition right if the data are collected for marketing purposes (under art. 14 b)

Having read this short notice on the default home page, the netizen should be able to choose an identifying cookie (like UserId=AZFD4309) or an anonymous cookie (like UserId=X[17]). In fact, this solution has been offered by Double-Click[18] but remains little used[19] because the common netizen is unaware of the cookies issue, and even more, of the invisible hyperlink phenomenon.

It becomes then very easy for the Web site to build a dedicated page for the access right of the data subject. While accessing to this dedicated Web page, the browser will communicate by in his header a identifying cookie, an anonymous cookie or no cookie at all. If no identifying cookie is sent, there is no specific information about the netizen. If there is an identifying cookie, then it is very easy to access to his specific information and to send him back into the dedicated access page.

1.6 The cookie’s weaknesses for the marketing

1. There has been a terrible jar when the cookie system has been denunciated by privacy organisations. However, the cookie in itself is not privacy killing, but due to the invisible and unfair way in which it has been widely used, he has been perceived as a symbol. Following a raising awareness of the netizen versus privacy on the Internet, a second cookie specification is under construction and will normally lead to a better privacy protection (RFC 2109).

2. By storing the identifier on each hard disk of each netizen, the cookie permits systematic authentication, but, at the same time, allow the informed netizen to modify, to exchange or to delete his own authentication. The databases of cookies stored will lose 90% of their marketing value if the identifier no longer refers to an existing cookie stored somewhere on a computer (for instance if a the computer disk crashes, if a new computer is bought or if a cookie killer program is used).

[17] To be effectively anonymous, all the anonymous users should have the same Id but also the same cookie duration. Otherwise, the cookie duration can be used as a unique identifier.

[18] http://www.doubleclick.fr/company_info/about_doubleclick/privacy/privacy2.htm

[19] between 5 to 10 opt-out procedures are daily recorded by Double Click, Gauthronet, op. cit., p. 94

3. Even if the cookie meta data fields[20] have been normalised, the critical VALUE field remains not normalised and it became very difficult for the cybermarketing companies to interconnect different cookie databases related to the same netizens to draw a global profile.

4. The data linked to the cookie are quite basic and do not reveal the revenues, the SSN, the physical or electronic address, the credit card number, the gender, the education or the family structure of the netizen. Even if those data have been collected by electronic forms and are stored in databases with an identifying cookie access key, there is no global data definition model permitting the exchange of this particular information.

5. The ultimate value added for the cybermarketing remains the interconnection of classical databases with virtual databases. But before doing this, it is important to get a unique identifier for all the netizens.

2 description of P3P protocol

2.1 P3P milestones

P3P is the anagram of Platform for Privacy Preferences[21]. They are many steps both at client and at server side to achieve a P3P complete process[22].

The netizen will have to fill in a form with some of his personal data like name, address, phone and fax number, SSN, CCN, gender, age, etc… Those data will be kept on his own computer. He will specify the purposes for which he will afford to communicate some of those data.

The Web site will have to fill a similar form indicating what kind of data he intends to use and for which purpose.

When accessing a Web site for the first time, the Web site will reveal his privacy practices, i.e. the data he wants to have and for which purpose. If this proposition matches with the privacy preferences of the netizen, the netizen browser will then send an acceptance notification identified by a pairwise or site ID (PUID), unique to every agreement the agent reaches with the service.

If the privacy practices of the Web site and the privacy preferences of the netizen do not match, some process of negotiation is foreseen but it is not quite clear how this negotiation will take place.

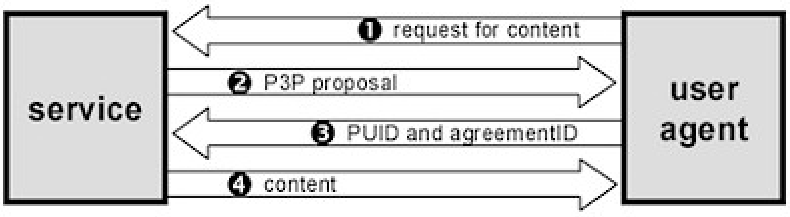
When accessing the Web site for the next time, the browser will systematically send this PUID in such a way that the Web site can know the privacy preferences matched between the netizen and the Web site.

[20] The duration, the path, the secure attribute and the domain allowed to get the cookie back.

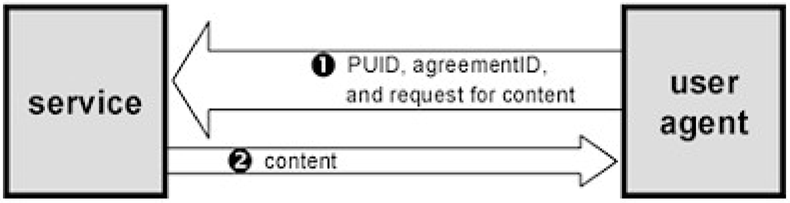
[21] The last working draft of the P3P protocol can be found on the W3C Web site at http://www.w3.org/TR/1999/WD-P3P-19990407 .

[22] Source : Joseph Reagle, Lorrie Faith Cranor, "The platform for privacy preferences", Communications of the ACM, Vol 42, No. 2 (Feb. 1999), Pages 48-55. Available as a W3C note at http://www.w3.org/TR/1998/NOTE-P3P-CACM-19981106/#anonymity

First-time visit to a service that requests PUID



Follow-up visit to a service that requests PUID



The basis of P3P is thus a *contract* between the user agent and a service.

2.2 P3P improvements.

Two others elements are cornerstones of the P3P protocol.

2.2.1 RDF

The first one is the use of the RDF[23] (Resource Description Framework) meta language. RDF provides interoperability between applications that exchange machine-understandable information on the Web. By using this meta language, the electronic agents will be able to use normalised data identifiers all over the Web. If widely adopted, this RDF meta format, can solve to problem of the cookie interoperability mentioned above.

2.2.2 APPEL

The second one is the ability for client software to download standard disclosures practices. The P3P Preference Exchange Language (APPEL[24]) offers the opportunity to define in a standardised format : "*Thus P3P includes a mechanism for exchanging recommended settings. These "canned" configuration files are expressed by APPEL, A P3P Preference Exchange Language. Rather than manually configuring a user agent, a user can select a trusted source from*

[23] Resource Description Framework (RDF) Model and Syntax Specification, W3C Proposed Recommendation, 05 January 1999, http://www.w3.org/TR/PR-rdf-syntax/

[24] W3C, "A P3P Preference Exchange Language (APPEL)", http://www.w3.org/TR/WD-P3P-preferences

which to obtain a recommended setting. These are the settings the user agent will use when browsing the Web on behalf of its user".[25]

3 How P3P can fulfil EU data protection directive requirements

3.1 Some European legal requirements for fair data processing

They are many fair data processing requirements based on EU directive 95/46[26] but we will limit our analysis on the following basis requirements :

- 4 b) the data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. (**legitimacy**)
- **4 c)** the data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed; (**adequacy**)
- **10)** the controller .. must provide ..:
  (a) the identity of the controller and of his representative, if any;
  (b) the purposes of the processing for which the data are intended;
  (c) any further information such as
  - the recipients or categories of recipients of the data,
  - whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,
  - the existence of the right of access to and the right to rectify the data concerning him (**information of the data subject**)
- **12 a, b,c)** Member States shall guarantee every data right to obtain from the controller: (a) without constraint at reasonable intervals and without excessive delay or expense:
  - confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,
  - communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,
  - knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in article 15(1);
  - (b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;
  - (c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort. (**Right of access**)
- **14 b)** Member States shall grant the data subject the right: (b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to

[25] Joseph Reagle, Lorrie Faith Cranor, op. cit.

[26] "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data" (published in the OJEC of 23 Nov 1995, L281, p.31).

third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses **(Right of opposition to marketing**)

- **25 1.-)** The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection (**Adequate level of protection**)

3.2 P3P as a fulfilment of EU data protection directive

EU directive requirement	*P3P requirement*
Legitimacy [art 4b]	P3P in itself offers no guarantee on the legitimacy of the processing
Adequacy [art 4c])	P3P in itself offer no guarantee that the data collected are necessary for the declared purpose
Information of the data subject [art 10]	This is the best added value of P3P. The netizen can a priori decide what kind of purpose are legitimate for him. In fact, depending on implementation, he will perhaps know the purposes of the Web site. The netizen also has the right to know the identity of the Web site rather then domain name located in the URL
Right of access [art 12]	P3P in himself offer no guarantee on the right of access
Right of opposition to marketing [art 14 b]	P3P in himself can reach this goal with the good client settings. One question remains. What will the Web site do if a visitor doesn't want to communicate his data for marketing purposes.
Adequate level of protection for transborder data flow [art 25])	P3P doesn't perform any check of the kind of data that can be transferred outside the European Union

It becomes very clear that P3P can achieve two steps towards better privacy practices, namely by providing a better data subject information and by granting a right of opposition towards direct marketing. However, the choice of a P3P compliant server will not be sufficient to grant the EU privacy compliance of a particular Web site. This is the sense of the opinion[27] expressed by the Group 29[28] which stated that : *“ 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.“*

[27] Opinion 1/98: Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS) : http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp11fr.pdf.

[28] Group of all European data protection authorities created by the article 29 of the Directive 95/46/EC

4 Conclusion

4.1 The P3P accuracy versus existing privacy killing technologies

The privacy killing implementation by the Internet industry of the HTTP protocol have been detailed in chapter 1. The question to be answered is to know if a P3P browser will reduce or not the HTTP chattering, the cookie phenomenon or the invisible hyperlinks outside the Web site visited.

The response to this question is negative. In fact the P3P protocol will increase the HTTP chattering, doesn't intend in itself to regulate the cookie problem and will not give to the user more control versus invisible hyperlinks, namely to cybermarketing companies located outside the European Union.

In fact, the single visible attempt to solve one of those three problems is the cookie opposition mechanism implemented in common browsers since version 3[29]. This attempt remains timorous and inadequate for many reasons :

1. The default setting is the most privacy killing and the average netizen doesn't know that the cookie is widely used by invisible cybermarketing companies to track every keyword typed on search engines.
2. The cookie blocking mechanism inhibit the reception of new cookies but doesn't prevent the systematic and invisible sending of cookies already received.
3. Some cookies are useful and not identifying (e.g. preferred language). Others are identifying but privacy compliant[30].
4. Several Web sites doesn't allow client denying cookies. But session cookies are much less privacy killing then persistent cookies. Refusing all the cookies can not be a global solution.
5. Several Web sites (or the Web sites invisibly hyperlinked) send many cookies and a case by case approach will cause a terrible click fatigue
6. In some cases, the cookie warning[31] is not fair but may scare the average netizen by arguing that he will receive less information if he refuses cookies. In fact, he will send less information about him in the future.
7. While installing a new browser, the first site (by default the Web site of the browser producer) to be visited can send a cookie before the user get the opportunity to deactivate the cookie feature.

Behind the P3P opinion mentioned above, the Group 29 has also produced a recommendation on Invisible Processing of Personal Data on the Internet[32]. By doing this recommendation, the Group intent to urge the Internet industry to produce privacy friendly software and hardware, and namely to give full data control to the user.

[29] Basically, three options are offered to the netizen : refuse all cookies, accept every cookie, see case by case.

[30] See above, point 1.5.

[31] In MSIE 4.O UK, the cookie warning stands as follow : "In order to provide a more personalised browsing experience, will you allow this Web site to put information on your computer ? If you click Yes, the Web site will save a file on your computer. If you click No, the current Web page may not display correctly." The courageous netizen has then to click on a new button to know the domain (not the sender !) of the cookie and his duration.

[32] Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware, available at http://www.europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp17en.htm

After being so deaf towards the W3C recommendation, will finally the Internet industry be receptive to the legitimate aiming of more privacy compliant products. The answer to this is two questions :

1. By who are the Internet browsers producers financed; by the data subject or by the merchants ?
2. Who has interest to get more privacy ?

4.2 The P3P as the privacy panacea

The P3P is sometimes presented as the solution to solve al the privacy problems on the Internet. It is a marketing argument that can not be verified.

P3P can effectively provide better data subject information (depending on the choice done at the implementation stage) or enhance opposition towards marketing processing. At the present stage, it is very difficult to appreciate the accuracy of P3P before knowing the default settings and the way in which APPEL configuration files will be promoted and distributed.

P3P will certainly not grant a global privacy compliance towards the basic EU data protection requirements in spite of the fact that it may cause this false impression.

P3P doesn't solve present problems like the presence and the content of many tens millions European profiles stored in New-York without the prior knowledge (and consent) of the data subjects. He will not bring an happy end to the cookie Jar or to the Intel PSN controversy.

4.3 The P3P as an enhanced cookie ?

In fact, it seems that the P3P has been conceived by the W3C, supported by the Internet Industry to palliate the weaknesses of the existing system of cookies for the cybermarketing industry while presenting this protocol as a privacy enhancing technology. It seems to be an argument presented by P3P specialists : " *P3P includes two identifiers that users can exchange with services in place of cookies*"[33]. Indeed that is the opinion expressed by the people who have given the "People's Choice" Orwell award to Microsoft Corp. for the Global User ID Number, Open Profiling System, and …the proposed P3P standard[34].

[33] Joseph Reagle, Lorrie Faith Cranor, op. cit., in Chapter "Anonymity and cookies".

[34] http://www.epic.org/alert/EPIC_Alert_6.06.html, point [6].