Law and technology convergence in the data protection field ? Electronic threats on personal data protection on the internet

Dinant, Jean-Marc

Published in:
E-commerce law and practive in Europe

Publication date:
2001

Link to publication

Citation for pulished version (HARVARD):
Dinant, J-M 2001, Law and technology convergence in the data protection field ? Electronic threats on personal data protection on the internet. in *E-commerce law and practive in Europe.* Wood Head Publishing, Cambridge, pp. 1-22. <http://www.crid.be/pdf/public/4223.pdf>

BUREAU VAN DIJK, MANAGEMENT CONSULTANTS (BvD)
CENTRE DE RECHERCHES INFORMATIQUE ET DROIT
FACULTES UNIVERSITAIRES NOTRE-DAME DE LA PAIX NAMUR (CRID)
CENTRO DE ESTUDIOS DE DERECHO E INFORMATICA DE LES ILLES BALEARS
UNIVERSITAT DE LES ILLES BALEARS (UIB)
GMD - FORSCHUNGSZENTRUM FÜR INFORMATIONSTECHNIK
INFORMATION TECHNOLOGY LAW UNIT OF THE CENTRE FOR COMMERCIAL LAW STUDIES
QUEEN MARY AND WESTFIELD COLLEGE (QMW)
INSTITUT FÜR INFORMATIONS-, TELEKOMMUNIKATIONS- UND MEDIENRECHT
WESTFÄLISCHE WILHELMS-UNIVERSITÄT (ITM)
NORWEGIAN RESEARCH CENTER FOR COMPUTERS AND LAW
UNIVERSITY OF OSLO (NRCCL)

CLIP
Electronic Commerce Legal Issues Platform

ESPRIT Project 27028

Electronic Commerce Legal Issues Platform

Law and Technology Convergence in the Data Protection Field ?

Electronic threats on personal data and electronic data protection on the Internet

Jean-Marc Dinant,
Centre de Recherches Informatique et Droit

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

1 Some privacy killing sides of the Internet Technology

1.1 The Intel Processor Serial Number

Since many years, the central processors units (CPU), the heart of the computer, have been identified trough a Serial Number written on the top cover of the chip. 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). What is new with the Intel Processor Number is that the Serial Number is not only on the top cover of the chip but is part of the electronic circuit of the chip itself. It means that a dedicated processor instruction can get his unique Id as a result of an instruction. This instruction can be included in an applet Java or in an Active-X control and then included in an HTML page. The PSN will then be transmitted to the Web site issuing the Web page containing the applet or the control. Technically speaking, the PSN can be disabled by turning off a particular flag. Intel claims that

- the flag will be turned off by default (in fact this depends of the BIOS[1] manufacturer's)

- the status of identification will be visible on the screen (e.g. on the task bar of Windows)(in fact this is the task of the Operating System builders)

- the PSN cannot be turned on without powercycling the computer. Some hacker organisations seem to have demonstrated that it was in fact possible to enable this number without turning the computer off and on[2].

A description of the Intel PSN controversy can be found on http://www.bigbrotherinside.com. According to Intel, the PSN will be used to identify users in electronic commerce and other net-based applications. Many privacy advocate organisations have protested and asked the FTC to oblige Intel to suppress the accessibility of the PSN via the Internet.

Intel has presented the PSN as an improvement for the Web security and as a secure identifier for doing E banking. Unfortunately, this PSN has not yet been used by any bank for such a purpose and security specialists like Bruce Schneier don't believe that the PSN is secure enough to provide such a requirement.[3]

[1] Basic Input and Output System. This is a basic program stored in a Read Only Memory and used during the startup of the computer. This program is the first one to be executed and will namely read the boot sector on the hard disk and load the first instruction of the Operating System installed on it.

[2] "*Pentium III serial number is soft switchable after all*" at http://www.heise.de/ct/english/99/05/news1/

[3] "As a cryptographer, I cannot design a secure system to validate identification, enforce copy protection, or secure e-commerce using a processor ID. It doesn't help. It's just too easy to hack." Cited in http://www.zdnet.com/zdnn/stories/comment/0,5859,2194863,00.html

1.2 Microsoft Global Unique IDentifier

At the beginning of March 99, the NY Times reported that a specific ID, called Global Unique Identifier (GUID), was systematically and automatically incorporated in each Excel97, Word97 or Powerpoint97 Document[4] [5]. In fact, it appears that this GUID was based on the identification of the Ethernet card installed on the computer. As a response, Microsoft has published on its Web site[6] two programs

- **Microsoft Office 97 Unique Identifier Patch** This patch, once applied will prevent the insertion of a unique identifier number in all new Office documents.

- **Microsoft Office 97 Unique Identifier Removal Tool :** This is a utility that can be used to remove the unique identifier from previously created Office 97 documents. Customers who are concerned about the presence of the unique identifier number can run the utility against one or several documents at a time.

Simultaneously, Microsoft announced that Office 2000 doesn't include the ability to insert unique identifier numbers in documents.

Following personal experimentation performed during October 1999, it appears that the two programs mentioned above require the installation of two "Services Release". The respective size of SR1 and SR2 are 8.683 Kb and 23.704 kilobytes, which represent about more then three hours of downloading time at the theoretical-never reached speed of 28.800 bit per second.

1.3 Browser chattering

Every surfer knows 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[7]

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-

[4] http://www.junkbusters.com/ht/en/microsoft.html#history

[5] http://www.techserver.com/noframes/story/0,2294,25591-41382-304399-0,00.html

[6] http://www.microsoft.com/presspass/features/1999/03-08custletter2.htm

[7] In fact, other data are such as the keep-alive or the host field can also be transmitted but their impact on privacy is weak or null, so they are not cited or explained below

			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[8] for HTTP 1.0 or in the RFC 2068[9] for HTTP 1.1. We can notice

- The first line is the only one 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 Powerpoint, 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. Microsoft reveal that the netizen is Belgian, French speaking.

The chattering phenomenon is not exclusively related to browser and appears to be a general practice of many Internet software like Email or FTP client or server programs.

1.4 Invisible hyperlinks[10]

Hyperlinks are the added value of Internet. They permit 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. In other 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.

1.5 Cookies

The cookies issues have already been widely discussed[11]. The SET-COOKIE is taking place in the HTTP response header[12], namely in invisible hyperlinks. If a duration is mentioned[13], the cookie will be stored on the netizen's hard

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

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

[10] 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.

[11] 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.

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[14], a cybermarketing company knows all the keywords typed by a particular netizen[15] 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[16]

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

The cookie permits a permanent, unique and systematic identification because it is systematically sent with every request of information. To the opposite, 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[17].

1.5.1 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[18], it means that before sending a SET COOKIE header, a Web site has to inform the consumer by communicating

a) his identity,

[12] 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

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

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

[15] 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 by data protection authorities as being personal data in the sense of art. 2 a) of the European directive 95/46.

[16] 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

[17] 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)

[18] "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).

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 happens 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[19]). In fact, this solution has been offered by DoubleClick[20] but remains little used[21] 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 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 or an anonymous cookie, then it is very easy to access to his specific information and to send him back into the dedicated access page.

1.5.2 The cookie's weaknesses for the marketing

1. 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 the major part 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).

3. Even if the cookie meta data fields[22] 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.

[19] 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.

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

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

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

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

1.6 Client-side scripting

Besides privacy harmful content lying in HTML code, the common browser can be instructed by the Web site to download and to execute content included in the HTML page. Those executable contents can be short listed as follows :

- JavaScript (available on MS Explorer and on Netscape Communicator)
- Java Applets (available on both browsers)
- Active-X controls
- Particular file format only readable by plug-in

The various security flaws detected and published on the Web will not be detailed here. For example, the Cuartango Hole[23] can be cited as a practical demonstration how a Web site can access to all the data stored on the physical or virtual hard disk of a netizen's computer. This hole has been tested by the author of this document and it appears to be effective. Many others security holes are daily published on the Web[24].

2 Privacy enhancing technologies

In this chapter, the so-called Privacy Enhancing Technologies are described and analysed. The basic idea of PETS is to protect the individual's privacy by using a technology against privacy-killing technology.

2.1 P3P

2.1.1 P3P milestones

P3P is the anagram of Platform for Privacy Preferences[25]. There are many steps both at client and at server side to achieve a P3P complete process[26].

[23] http://pages.whowhere.lycos.com/computers/cuartangojc/cuartangoh1.html

[24] By instance : http://www.ntbugtraq.com , a Web site only dedicated to the security flaws of NT systems.

[25] 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 .

[26] 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

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 is willing to communicate some of those data.

The Web site will have to fill in 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.

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

The RDF[27] (Resource Description Framework) metalanguage provides interoperability between applications that exchange machine-understandable information on the Web. By using this metalanguage, the electronic agents will be able to use normalised data identifiers all over the Web. If widely adopted, this RDF meta format, can solve the problem of the cookie interoperability mentioned above.

The P3P Preference Exchange Language (APPEL[28]) offers the opportunity to define disclosures practices in a standardised format. Many Web actors will thus be able to provide typical disclosures practices. "*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 which to obtain a recommended setting. These are the settings the user agent will use when browsing the Web on behalf of its user*".[29]

2.1.2 P3P adequacy vs European Directive requirements.

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

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

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

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

the opinion[30] expressed by the Group 29[31] 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.“*

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 this recommendation, the Group intent to urge the Internet industry to produce privacy friendly software and hardware, and namely to give to the user full control over his personal data and profiles.

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 forsee an access right
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

2.1.3 P3P : a privacy killing or enhancing technology ?

The P3P is sometimes presented as the solution to solve all 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.

[30] 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.

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

[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

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.

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. 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.

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

P3P has been conceived by the W3C, supported by the Internet Industry also perhaps 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]. P3P : a enhanced cookie ? This 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].

2.2 Cookies killers

To solve the cookie's privacy issue, two kinds of reactions are analysed below. The first one originates from the Internet industry itself and has been incorporated into the main browsers on the market. The second reaction came from various privacy activists or software houses. It consists in tools permitting to delete all or some of the cookies.

2.2.1 The cookie opposition mechanisms implemented by the industry

In fact, the single visible attempt to solve one of those three problems (browser chattering, invisible hyperlinks, cookies) is the cookie opposition mechanism implemented in common browsers since version 3. It is possible for an aware netizen to parameterise the browser by choosing

- to accept every cookie
- to refuse every coookie or cookie not sent back to the originating server (Netscape)
- to be asked on a case by case approach

This attempt remains timorous and inadequate for many reasons:

[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].

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 inhibits 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[35].
4. Several Web sites doesn't allow client to deny cookies. However, session cookies[36] 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[37] 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.

2.2.2 Independent programs

Some of these programs can be found on http://tucows.belgium.eu.net/cookie95.html . Cookie *washer*, cookie *cutter,* cookie *master* or cookie *cruncher* are some of the freeware or shareware programs that every netizen can download and use on the Net. Similar remarks to the above section apply:

1. The netizen has to process daily its own cookies files on a case by case approach because some cookies are not identifying or are privacy compliant.
2. In the case of shareware programs, the netizen has to pay to protect himself (privacy for the rich)
3. The cookies handling mechanism remain not straightforward even for a computer specialist (privacy for the clever ?)

2.3 Proxy-servers

The proxy server is an intermediary server between the netizen and the Net. He is acting as a Web cache, improving drastically the performance of the Internet. Many big organisations or Internet Access Providers have already implemented such a solution. Each page, each image or logo downloaded from outside by an organisation's member is stored on a cache and will be instantaneously available for another member of this organisation.

It remains no more necessary that every member of the organisation located before the proxy server own his own TCP/IP address, just because they do not directly access to the Internet. Furthermore, the proxy server will normally[38] not transmit the TCP/IP address of the netizen to the Web site and can filter the browser chattering. Because a proxy server handle the HTTP protocol, the cookies stored in the HTTP header can therefore easily be removed, changed, or… stored by the proxy server. In fact this solution brings many advantages because it doesn't kill any advertising,

[35] See above, point 1.5.

[36] Cookies with no duration mention will not be stored on hard disk but only into the RAM memory

[37] 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.

[38] Unfortunately some proxies are adding in the HTTP header the TCP-IP address of the PC they are working for.

necessary for the financing of some Internet services like search engine. It permits a "one to many" marketing strategy towards a aggregate of many persons working in the same organisation (or department, depending on the place and the amount of proxy installed; it is possible to install many proxies in cascade).

2.4 Anonymising services

Good examples are the anonymiser[39] or the "zero knowledge system[40].

The **Anonymiser** present itself has being able to

- Act as a intermediary between you and sites you visit, concealing your identity from invasive tracking measures
- Block hostile Internet programs embedded in the Web page (Java and JavaScript) that may damage your computer or gather sensitive personal

The netizen has to pay to take benefit from anonymous services: $14.99 for 3 months, $49.99 for one year. The netizen has always to connect to the Anonymiser Web site to use the anonymising services. It means that this service remains very vulnerable to surveillance by the police or the government. The Anonymiser can provide anonymous services such as surfing, mailing or file transfer.

Technically speaking, the Anonymiser is acting as a proxy server and will hide the HTTP browser chattering and the TCP-IP address of the surfer.

The main problem while using this service is that you have to trust to a particular company and that this company will be aware of what you're doing on the Web.

The **zero knowledge system** proposes a *software* called "Freedom". This solution is based on at least three TCP/IP relays combined with heavy (at least 128 bits) encryption. Because the TCP/IP is used by every service on the Net, every service is thereby encrypted and anonymized. Each of the three TCP/IP intermediary stations knows only the TCP address of the predecessor. They keep no logbook in such a way that even two relays put together are unable to trace back the information asked or retrieved. Of course, the routing of the information is dynamic and will be likely to change even during a very brief communication. A cookie management system seems to be integrated to Freedom. The software is a beta version and the final price is not yet known.

2.5 Infomediaries

In this solution, the netizen will chose an infomediary[41]. "*An infomediary, or information intermediary, is a trusted person or Web-enabled organization that specializes in information and knowledge services for, about and on behalf of*

[39] http://www.anonymizer.com/3.0/index.shtml

[40] http://www.zeroknowledge.com

[41] http://www.fourthwavegroup.com/Publicx/1635w.htm

a virtual community. The infomediary facilitates and stimulates intelligent communication and interaction among the members of the virtual community. It administers and cultivates a proprietary knowledge asset that contains content and hyperlinks that are of specific interest to the community. In accordance with the privacy constraints that are mandated by the virtual community, the infomediary gathers, organizes and selectively releases information about the community and its members in order to fulfill the needs of the virtual community…"

An infomediary company will not sell individual data but will act as an agent to search the better bargain on the Net. Furthermore, in many cases, an infomediary company can also purchase the wanted good or service and deliver it to the final consumer while leaving him in the darkness of the anonymity.

The infomediary company can also provide intelligent agents to help the subscribers to accomplish their task. In this case the way in which the personal data will be handled

2.6 The labellisation of privacy

The labellisation consist of a quality stamp put on the Web site. Since many years, various privacy labels have appeared: Trustee[42], Privaseek[43], the Better Business Bureau[44], WebTrust[45] are such labelling systems. They are at least two main problems raised by the privacy labellisation.

The first one is the label content. Very often, the simple the label content is far below then the European DP requirements. The concept of notice and choice is certainly not sufficient. The right of access, the data minimisation principle, the right of opposition, the principle of legitimacy and proportionality, the obligation to notify to the national data protection authority are some of the corners stones of the European data protection principles. The main social risk is to assist to the widespread dissemination of various privacy labels in Europe. These labels will not necessarily bring any serious guarantee to the data subject while giving to the data controllers this false impression.

The second problem lies in the control of the Web site privacy practices. Many kind of controls can be envisaged. The major concern lies in any questions

- Who will do the control (i.e. how, with which empowerment from the controlled company,…) ? In the worse cases, it appears that the controller will be, in a first instance, the data subject himself, with all the difficulties to identify the privacy inadequacy with the posted practices, to prove it and to report it to the label controller.

- Who will pay ? Due to the fact that labelling are privy initiatives and doesn't benefit from government financing support, the labelling organisations will always, less or more be under the pression of the companies that they are supposed to control

[42] http://www.trustee.org

[43] http://www.privaseek.com

[44] http://www.bbbonline.org/businesses/privacy/index.html

[45] http://www.cpawebtrust.org/consumer/index.html

- What will be the sanctions if any ?

The underlying problem with labellisation is linked to the fact that all the powers lie in the same hands: the label content definition, the label attribution and withdrawal, the auditing of the company remains widely often managed by the same actor. Because there is no "common" law just like in Europe, every labelling organisation has his own interpretation of privacy. Because the financing system is not due to the government, those labelling companies are paid by the companies they are auditing; a true independence remains hypothetical.

The Trustee case is a good illustration of not solving those problems. Among many thousands of complaints, two complaints have been made public, primarily not by the Trustee organisation but by the Junkbuster[46] association which was the plaintiff.

The first complaint was linked to the Windows 98 online registration wizard. During this registration, it happens that the customer has the choice to send or not details about the installed equipment installed on the PC. Whatever can be the choice made by the customer, it appears that the detail of installed equipment was always sent by the registration wizard[47].

Event "*if TRUSTe believes that is important to note that the transfer of Hardware IDs to the Microsoft secure server without customer consent did, in TRUSTe's opinion, compromise consumer trust and privacy*[48], Trustee has considered that *" TRUSTe has determined that Microsoft.com was in compliance with all TRUSTe principles*"[49]

What would have happen if Trustee has come to the conclusion that the Trustee principles ? " *Had TRUSTe determined that Microsoft.com had violated its stated practices, TRUSTe would have conducted an audit to ascertain that sufficient remedies had been put in place.*"[50]

The idea has circulated on the Web that such a decision was due to the fact that "*Microsoft is a premier sponsor of TRUSTe and a member of the TRUSTe privacy program, an independent, non-profit initiative"*[51].

This story is not anecdotal. During the online registration process a so called HWID (HardWare Identification) number was sent to Microsoft. This HWID number shares one common identifying part with the GUID described above. Thanks to this ID which is the Ethernet controller world around unique number, Microsoft was[52] able to identify the author of every Word, Excel or Powerpoint document attached by Email or available on the Web. It is sufficient for the author of the document to have filled the registration form with the Windows 98 wizard to be identified by Microsoft.

[46] http://www.junkbusters.com

[47] http://www.truste.org/users/ms_process.ppt

[48] http://www.truste.org/users/users_w1723.html

[49] ibidem

[50] ibidem

[51] http://www.microsoft.com/info/privacy.htm

[52] is still, unless those data have been destroyed.

Beside the privacy aspects, this will represent a bulk and unfair advantage on every competitor building Operating Systems. By systematically gathering equipment information on the maximum number of computers, Microsoft is able to know the average installed base of various equipment peripherals or add on cards and is therefore able to propose the most strategic drivers[53] programs[54].

Furthermore, it permits to Microsoft to detect pirated software easily. If an Office97 document available on the Web does not include a GUID related to a registered user, then it is very likely that this document has been produced by an illegal copy of an Office 97 program. This provide a second advantage towards competitors who will not be able to made a difference between a document produced by a legal or illegal copy.

2.7 Why is the surfing so privacy killing ?

The combination of browser chattering, invisible hyperlinks and cookies permit invisible profiling of every individual net user using a browser as installed by default. This profiling is not "per se" linked to the HTTP protocol, as it has been defined by the W3C[55]. Even more, the HTTP 1.1 protocol definition has explicitly drawn the attention of the industry to possible privacy attempts while doing the implementation of the HTTP protocol[56]:

- "*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[57] 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.

[53] programs delivered with the OS and permitting to the OS to interoperate with an external device or an add on card

[54] http://www.microsoft.com/ntserver/nts/news/msnw/LinuxMyths.asp : "*Linux does not provide support for the broad range of hardware in use today; Windows NT 4.0 currently supports over 39,000 systems and devices on the Hardware Compatibility List".*

[55] 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 produces non-mandatory but de facto normalisation intended to guarantee the interoperability of computers on the Internet. In fact, it appears that the HTTP protocol

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

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

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.

Even if the client programs like the browsers (having newsgroup, file transfer, email and surfing capabilities) are distributed for free, their conception is very much more complicated than the setting up of equivalent server programs. Such servers are not distributed free to the companies. E-commerce companies are paying for the distribution, at a world wide level of a very specific client-server technology. This technology is not designed to preserve the privacy of the netizen, only perceived as a possible customer that must be profiled as much as possible.

3 Conclusion : A Paradigm Shift in the Data Protection of the Consumer

3.1 Identified, identifiable and anonymous individuals

I will not enter the debate of identifying what kind of information are private and what kind of information isn't. What can be considered as an axiom is that privacy is a personal feeling. So does the general data protection directive 95/46 CE[58]. It doesn't define what is privacy but only creates rights for the data subjects and duties for controllers when personal data are processed. The problem then lies in the definition of personal data. Following art 2 (a) of the DP Directive: *'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*. Recital 26 of the DP directive add that " *to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person".* On the Internet, this means that if a data controller knows an identification number, one or more specific factors related to the economic, cultural or social identity of the individual who is behind the screen, this individual is identified.

The Internet network is based on the TCP/IP protocol. Every netizen is transmitting this TCP/IP [59] address while using a service on the Net. The TCP/IP addresses range are attributed on the world level[60] to IAP. Those addresses are then sold or hired to organisation or individuals. By using a public service like http://www.ripe.net/cgi-bin/whois it is always possible to identify the responsible of a particular TCP/IP address attribution. Typically, this responsible will be

[58] 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). Full text is available at http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html

[59] This is linked to the nature of the TCP/IP protocol. TCP/IP is a packet switching, connectionless protocol. Every information packet incorporates the TCP/IP address of the sender and of the recipient.

[60] The Internet Corporation for Assigned Names and Numbers (ICANN) is the non-profit corporation that was formed to assume responsibility for the IP address space allocation (http://www.icann.org). In Europe the addressing space is managed by the RIPE organisation (Réseaux IP Européens) (http://www.ripe.net)

- the manager of a Local Area Network linked with Internet (e.g. : a SME or a public administration). In this case, he will probably use fixed IP addressing scheme and keep a list of correspondence between people's computers and TCP/IP addresses. If this responsible is using the Dynamic Host Configuration Protocol (DHCP[61]), the DHCP program will typically keep a log book where the Ethernet card number will be written. This world around unique number identify a particular computer in the LAN.

- A Internet Access Provider having a contract with a Internet subscriber. In this case, the IAP will typically keep a log file with the attributed TCP/IP address, subscriber's ID, date, time and duration of the address attribution. Furthermore, if the netizen is using a public telecommunication network (mobile or residential phone), the called number will be registered by the phone company for billing purposes

In both cases, this is to mean that a third party, well and easily knowable by the Internet, can identify (i.e. knowing the civil identity (name, address, phone, …)) the netizen by using reasonable means.

An IP address is a world around unique number related to one computer at a certain moment[62]. Due to the nature of the Internet network, this TCP/IP address (a unique number) will always be sent to each visited Web site along with the name of the page requested. By default, most of the Web servers will store in a logfile, at least

- TCP-IP address

- Date and time of the request

- Full name of the page requested (including parameters like keywords to be searched)

- … More personal data are sent in the HTTP header and can be added in the logfile.

By cumulating the browser chattering and the invisible hyperlink effects, all the advertising agencies will get the same information vs the Internet pages on which they are uploading ads in real time.

DoubleClick, one of the big cybermarketing agencies[63], made a big difference between non-personally identifiable information and personally-identifiable information[64]. Following DoubleClick assertions, only non-personally-identifiable information is processed by the agency. Unfortunately, this distinction doesn't match the legal distinction made by the Directive 95/46 between personal data and anonymous data for two distinct reasons.

[61] The Dynamic Host Configuration Protocol (DHCP) is an Internet protocol for automating the configuration of computers that use TCP/IP. DHCP can be used to automatically assign IP addresses. (http://www.dhcp.org)

[62] Whatever can be the duration of the address assignment. Even if it is a dynamic address, this address is an identifying number at least during the duration of the Internet connection of the netizen.

[63] more then 500,000,000 advertising banners sent each day : http://www.doubleclick.net/company_info/investor_relations/financials/analyst_metrics.htm

[64] http://www.doubleclick.net/company_info/about_doubleclick/privacy . : " *DoubleClick does not collect any personally-identifiable information about you, such as your name, address, phone number or email address. DoubleClick does, however, collect certain non-personally-identifiable information about you, such as the server your computer is logged onto or your browser type (for example, Netscape or Internet Explorer).*"

If not hidden by a non chattering proxy server, the TCP-IP address of the netizen is always sent to DoubleClick. As explained above, in most of the cases, this TCP/IP address will enable an intermediary to identify one particular person.

Even if the TCP/IP address is hidden by a privacy compliant proxy, an identifying cookie originally sent by DoubleClick has been stored by default by the browser on the netizen hard disk. This cookie will be sent back to DoubleClick before each time an advertising banner is uploaded on the screen of the netizen. This cookie is an " *identification number"*. This number is associated, in DoubleClick's database, with a list of various data like[65]

1. The country where the netizen lives
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. Internet Access Provider
7. Typology of Web sites currently visited
8. The keywords typed on important search engines
9. Some of the Web pages visited
10. The browser used by the netizen
11. The brand and type of the OS used by the netizen
12. …

which are undoubtedly "*factors specific to the ... economic, cultural or social identity"* of a particular netizen.

In the specific case of DoubleClick, it is important to notice the recent merging between this company and Abacus, a "*cooperative membership database, contains records from more than 1,100 merchandise catalogs, with more than 2 billion consumer transactions from virtually all U.S. consumer catalog buying households"*[66]. Technically speaking, it was sufficient for DoubleClick to advertise on a Web site owned by Abacus to be able to merge, one a one-to-one basis, "anonymous" profiles with particular customers of Abacus.

3.2 The E-Commerce privacy paradigm shift

When I was a child, my parents always looked at the door of the store they were intending to come in to check if there was an "entrée libre" label. The meaning was that in the stores showing this label it was possible to simply visit without buying anything. Nowadays, it seems clear to everybody that it is possible to exit a supermarket without any purchase.

Privacy is not only a set of legal rules described or not in a text of law, but firstly a modus vivendi, social rules unanimously known and applied both by the client and the merchant. Nowadays, it seems clear that anybody can visit a store and even purchase some goods without systematically leaving any trace (if he pay cash). Nowadays, the advertising banners visible in the stores don't remember who was reading their message and where he does come from.

[65] 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

[66] http://www.abacus-direct.com

Let’s have a look at what happen on a standard computer (i.e. equipped with a Intel Pentium III and with a common browser installed by default) to the “netizen on the street” who enters a E-commerce Web site.

The car the customer is using (brand, age, color = operating system type, type of processor), his equipment (browser’s type, version, subversion, is MS Office installed or not ?), the language he speaks and the place where he has found the store address (the referring page; see above) are systematically and imperceptibly communicated to the store manager on an electronic, easy to process form. It seems unclear if the store manager has the ability to read the frame serial number (=Pentium Serial Number) but this possibility is not to be excluded. The store manager can seamlessly stick an identifying bar code under the bumper of the car. He will record all the motion of this particular (identified by a bar code) customer, the goods he looks at, the goods he doesn’t look at, the goods that he will put in his shopping basket and the goods that he will put back in the right (?) shelves.

The advertising company knows in real time all the data above (thanks to the browser chattering that is the same towards both Web sites voluntary visited and Web sites invisibly linked). The advertising company can stick his own bar code (cookie) under the bumper of the car. This will allow the recognition of this particular customer if he enter to another shop where this company is advertising. It will choose in real time the banners that will be posted just before the customer will enter a particular department. It will notice what are the banners interesting the customer and add all those data to the customer anonymous profile.

This is not a fiction, but what happens seamlessly and daily to many tens millions of European netizens on the Web. The main problem underlying the privacy on the Web is that the way in which the electronisation of the commerce has been performed constitutes a radical change in a social privacy consensus between consumers and merchants. Even if this has not been the original, deliberate or conscious purpose of the merchants, the technology that has been widely implemented by the Internet industry is radically modifying, at least at the privacy point of view, the socially accepted way in which customer and commercial companies exchange and share personal information.

By doing this kind of domestic-economic-electronic spying, E-commerce and advertising companies as a whole are in the long term promoting mistrust on the Web. Even if they are widely used, those spying techniques remain hidden in the darkness of the millions of code lines of browsing software. In most of the cases, they are brought to light by chance, echoed and amplified on various media. There is a rising risk of generating a privacy paranoia that will keep netizens away from the Web even if the privacy killing risks suddenly disappears or significantly decreases.

4 Recommandations

4.1 The dead-end of individual Privacy Enhancing Technologies

We have shown that in privacy killing technological environment, the are various solutions permitting to an aware rich and clever user to protect himself against various but well determined risks. We do not consider that this solution is the best solution. It may be compared to the distribution of gas mask to solve the air pollution problem or of bulletproof jackets to reduce the criminality. Of course, even if those equipment’s are be distributed free (it is not the case for all privacy enhancing technologies), the will probably be in a short-term view a significant decrease of dead by inhalation or crimes. In the long term, there will be a rise of the air pollution (why reduce the air pollution if everybody is protected?) and probably the apparition of enhanced killing guns able to go through bulletproof jackets.

This solution is not a long-term solution. Furthermore, a subtle perversion exists in this promotion of individual privacy enhancing technologies. Suddenly, the data subject is no more protected by law enforcement but has to continuously protect himself by buying, installing, controlling and maintaining technical knowledge. The Directive 95/46 clearly puts some obligations on the shoulders of processors, not on the shoulders of the data subjects. Just because, in the European Union, privacy is fundamental human right that belongs to the public order and must therefore be granted to every European netizen, poor or rich, clever or not.

4.2 Where are the privacy-enhanced technologies?

The very brief privacy auditing of current Internet technologies has demonstrated that many privacy killing features have been put (and hidden?) in various popular programs, not by necessity but by choice of the Internet industry. It is amazing to observe that many fundamental privacy-killing features (like the GUID of Microsoft or the presence of cookies in invisible hyperlinks) have been discovered by chance. How many other privacy-killing features are still hidden into the depth of millions of computer code lines?

Whenever such features are made public, the industrial response is inefficient. For instance, to solve the GUID problem, the conscious netizen may have to spend many hours to download efficient patches. The cookies warning features as implemented in version 4 of the most popular browsers remains unusable. The default is always the most privacy-killing. Etc.

What is dramatically missing in the European Union is a technological and a priori control on the importation of privacy killing software. It remains utopia to believe that efficient control on data protection on information “highways” can be reached without controlling the software (=the cars) used to accomplish personal data transfer. The netizen is acting as a push button agent, still believing that he controls his data while some data transfer are seamlessly happening under the remote control of the authors of the software.

The underlying problem to this idle talk of the Internet industry can perhaps be found in the indirect financing of free browsers by the merchants. As long as the netizen in the street will not be aware of the privacy killing features hidden in the common browsers, he will be unable to produce a valid choice, even if the privacy seems to be a major criteria of his personal choice.

4.3 The IAP as a infomediary

Opposed to the Internet industries, the Internet Access Providers are mainly paid by the data subjects. Contrasting with the data subjects, they have the technological knowledge to understand the privacy killing features hidden in the software agents[67]. A proxy-server is today an industry standard feature widely used to spare bandwidth. Some proxy-servers[68] can be configured to filter browser chattering, cookies and invisible hyperlinks and hide the original IP address of the data subject. In such a way, anonymity can technically be reached.

At a first glance, this privacy compliance does not bring any advantage to the IAP. *"Companies playing the infomediary role will become the custodians, agents, and brokers of customer information, marketing it to businesses (and providing them with access to it) on consumers' behalf, while at the same time protecting their privacy".*[69]

In the actual cybermarketing model, profiling is performed by invisible companies without the knowledge (and therefore without the free consent) of the data subject. The personal data coming from different sources are merged to form a global privacy profile that can then be sold.

In the model of the infomediary, every ISP or Web site will act as an anonymising service to keep for itself the benefit of marketing. He can propose Intelligent Agent Software to the customer, negotiate for mass buy, directly advertise towards the customers, etc…

This model will generate new opportunities and new revenues for European Internet companies and will avoid the risk of centralisation of personal data outside the European Union.

4.4 The mutual recognition of Internet Software as a significant component of telecommunications terminal equipment

The Directive 1999/5/EC on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity define (art. 2 (b)) a telecommunication terminal equipment as a "*product enabling communication or a relevant component thereof which is intented to be connected directly or indirectly by any means whatsoever to interfaces of public telecommunications networks".* A browser can thereby be considered as a telecommunication equipment.

The same directive states that *the Commission may decide that apparatus*[70] *...shall be constructed that it (c) incorporates safeguards to ensure that the personal data and privacy of the user or of the subscriber are protected".*

[67] We will not develop here the concept of Intelligent Software Agent while this notion tends to evaluate but appears nowadays as one of the best way to produce anonymising and added value services on the Web

[68] So is, for instance, the free proxy-server proposed by JunkBuster (http://www.junkbuster.com/ijb.html)

[69] Who Can Be an Infomediary? John Hagel III and Marc Singer (Adapted from Net Worth: Shaping Markets When Customers Make the Rules, Harvard Business School Press, January 1999), http://www.hbsp.harvard.edu/ideasatwork/hagel_singer.html

[70] Note of the author : following art. 2 (a) an "apparatus is namely a telecommunications terminal equipment"

4.5 EU must promote law and technology convergence.

The best way to do that is to promote dialogue between lawyers and computer scientist. At the first hand, it appears that the national data protection authorities have a weak technological background. At the other hand, it seems clear that privacy issues raised by various Internet technologies were foreseeable but have been neglected by the industry.

Let's take one concrete example. In the Intel Pentium III case, a less privacy killing way was to include not a serial number identification instruction, but a serial number verification instruction. In the first scenario, an active component[71] is able to get the PSN. In the second case, the active component is only able to check is a serial number *freely given by the netizen* is the exact serial number of the installed processor. The authentication function of the PSN is preserved while the privacy killing aspect is widely reduced. This is only a suggestion but it seems me clear that it is almost always possible to reduce privacy killing side effect while keeping technological efficiency, if the privacy requirements are put in the product specification at the very beginning. If the privacy concern is not taken into account, the only solution is to build so-called privacy enhancing technologies that protect the clever and the rich. This is a time and resources consuming process which largely contributes to maintain mistrust on the Web.

The next two technological privacy issues are the P3P protocol and the new Ipv6 protocol which will permit to each netizen to get a personal static IP address for his whole life.

[71] like an Active-X control or a Java applet