The concepts of identity and identifiablity

Dinant, Jean-Marc

Published in:
Reinventing data protection ?

Publication date:
2009

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

Chapter 5
The Concepts of Identity and Identifiablity: Legal and Technical Deadlocks for Protecting Human Beings in the Information Society?

Jean-Marc Dinant

5.1 The Protection of Data as Seen by Computer Science

Generally speaking, technology in itself does not deal with personal data and even not with privacy but rather, from the very beginning, with data security, wherever those data may concern a human being and wherever this human being is identified or identifiable. Originally and during many decades, the security conception in the field of the information technology has been based on three corner stones: integrity, availability and confidentiality of information systems.

Recently, the identification and authentication of users has appeared as a new requirement for security. Roughly speaking, this authentication does not claim to be, in se, a corner stone of ICT security but rather a means to achieve the integrity, the availability and the confidentiality of information systems. In fact, to permit an assessment of the security of an information system, it may be useful to log all the transactions that may compromise the availability, the integrity and the confidentiality of the information system. In an insecure virtual world, populated by bugs and hackers, such a systematic collection of the traffic can make sense. Behind the identification of users, the authentication becomes more and more crucial in a virtual world in which a continuously growing amount of transactions between bodies and relations between humans do not involve the simultaneous physical presence of the implied parties and where a wide majority of information systems can be reached through the Internet by everybody in the world in real time, without needing to enter in a geographically delimited area.

The general requirement for user's authentication and identification has lead to a new branch inside information security: the so called Identity Management Systems. In this context, the wording "identity" does not relate to a philosophical or legal notion but rather to a kind of management of rights granted to particular identified and authenticated users within an information system. The assessment of the security of an information system can not be achieved without an infrastructure of rights

J.-M. Dinant (✉)
Technology and Security Research Unit, Centre of Research in IT and Law, University of Namur, Namur, Belgium
e-mail: reinventingprivacy@dinant.org

S. Gutwirth et al. (eds.), *Reinventing Data Protection?*
DOI 10.1007/978-1-4020-9498-9_5,

management describing who can access to what (availability), who can not access to which kind of information (confidentiality) and who has the right to modify which kind of information and in which circumstances (integrity).

In this framework and since many years, log files have been structured, deployed and enabled by default in each kind of information server (HTTP, FTP, RAS, SMTP, POP, SQL, etc.). Those log files have been originally designed for debugging purposes and, in this context, every information related to the request and the requester – including but not limited to – date and time, IP address, identification of the user, his location, the device used, the operating system of the device, the brand and version of the client software, etc may be relevant and becomes thus collected and stored. This is to say that, on the Internet, every client device communicating with a server (this is done daily by reading a web page, placing a post on a blog, sending or receiving a mail, chatting, etc) by default and systematically leaves numerous traces at the server side. Those traces are stored in log files and those log files may, in their turn, be archived in data warehouses. The huge amount of traffic data stored in data warehouses is currently more and more exploited, for a new purpose having no link with security requirements or debugging purposes. After many months or years, those traffic data are, in their huge majority, electronic evidence of perfectly legal (trans)actions that do not bring any substantial added value to the preservation of the availability, the confidentiality or the integrity of modern information systems.

Nowadays, predictive analytic modelling rises up as a new discipline combining data mining and statistics to build behavioural modelling of users. Both due to the raising performance of processing (in terms of speed and algorithmic progresses) and the endless rising capacity of massive data storage, it becomes now possible to apply single pass algorithms to several millions of individual transactions to extract a typical behavioural model of users in a few hours or days. The techniques used for weather forecast on the basis of a thousand observations can now, technically speaking, be applied to millions of human transactions and are used to predict human behaviour rather than weather, with a reasonable range of error.

Three characteristics of such a massive human data analysis need to be underlined.

- First of all, the predictive modelling does not use human common sense. A predictive model while being applied to an individual, permit, on the basis of certain characteristics of his past history to predict characteristics of his behaviour in the future. This modelling is the result of computation and not of reasoning. The modelling can predict what will probably happen but is totally unable to explain why a given individual will have this or that kind of behaviour. There is no semantic in predictive modelling. Even if human reasoning may instinctively take place in the mind of a human being facing predictive modelling's results.
- One may be feared while remembering the fable of Jean de la Fontaine "the wolf and the lamb". This lamb was desperately arguing that he was not guilty. After having admitted that the lamb was not guilty, the wolf falsely asserts that it was his brother's fault. While becoming aware that the lamp does not have any brother, the wolf concluded that it should have been the fault of someone of the lamb's family. Jean de la Fontaine thereby explains that the law of the strongest is always the best. And this law permits the wolf to eat the lamb without any further jury. Predictive modelling can produce an automated decision about an individual on the basis of what others have committed. Commercial decisions like contracting, revolving a contract or fixing a price do not need to be motivated.
- Predictive modelling, even if processed versus harmless data may lead to highly sensitive information, by side effect, just because there is no semantic control of the modelling. We have been told about a particular data mining result into bank transactions. From the data analysis of an important group of customers of a bank, rises up a profile of rich individuals starting to sell all their auctions without any link with their competitiveness. The analysis software has put the emphasis on the correlative link between this particular profile and the date of the death of those individuals. This strange behaviour was mainly originating from rich individuals in the few months before their death. The data mining process was in fact identifying and isolating the very typical profile of rich human beings who know that they have contracted a fatal disease and have urgently decided to distribute their economies to their family and friends. The bank has now a technical tool, seamlessly applicable to all their customers, that will permit to identify, with a minor range of error, the fact that particular customers know that they will die in the following months. This information may be considered as totally intrusive. It is not to say that this information is irrelevant, notably in the case in which the bank also deals with life insurance.

Industry and DPA does not agree on the point of knowing if anonymous traceability constitutes a personal data processing or not. Since many years, user's privacy has been a raising concern among telecommunication engineers but the actual widespread of security embedded in ICT remains symbolic.

The EC do not need new legal tools but may take immediate action, namely on the basis of Art 3 & 5.2 of EC Directive 99/5 and Art 15 of the EC Directive 2002/58. It is worrying to note that, in a recent communication of May 2007, the EC is looking for an intervention of the Parliament and the Council and is, for instance, still desperately emphasing P3P, a privacy inefficient protocol invented in 2002 and implemented since then by less then 5% of the web sites and unsupported by Firefox, Opera or Safari.

The technical knowledge of privacy advocates, consumer's organisations and even of the European Commission remain stable while the technology is becoming more and more subtle and seamlessly intrusive. As a concrete result, wide spreading of transclusive hyperlinks and continuous and individual monitoring of Internet users is nowadays the rule while non surveillance appears to be one exception. In the following sections, we will briefly analyse and remind actual problems and how they have not actually been resolved.

5.2 The Withdrawal of the PSN Number

Privacy advocates will never forget the PSN story in 1999. After having input an electronic serial number into their Pentium III processors and after many months of pressure originating from privacy advocates, Intel decided to withdraw this number. Since the very beginning of the hardware industry, the central processors units (CPU), the heart of each personal computer, have been identified by mean of a Serial Number written on the top cover of the chip. Intel announced on January 1999 that they were 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 was 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 obtain this unique ID. This instruction can be theoretically included in a script at the client side incorporated in a web page. The PSN can then be used as an identifier to trace a particular user, just like a cookie.

Due to public pressure and namely to a parodist web site called www.bigbrotherinside.com, Intel decided to withdraw this PSN from the central processor and the Pentium IV from Intel did not include this PSN any more.

Unfortunately, the vast majority of substantial parts of a computer, at the exception of the central processor, i.e., among others, all USB devices like mouse, keyboards, printers, modems, stick and RAM memories, memory cards, network cards, motherboards, hard disk and last but not least, RFID's and so on do include such an electronic identifying number.

Furthermore, a few months ago, Apple has included in all their new Intel based Macs a TPM chip that identifies and authenticates a single Apple computer through solid cryptographic means. This fact, even if published by the press, has not triggered any substantial reaction

5.3 Many Billions of Transclusive Hyperlinks Per Day by Google and Co are Widely Superceding the Echelon Monitoring Capacities

According to Wikipedia, transclusion is "*the inclusion of the content of a document into another document by reference*". The transclusion can be made at the server side or at the client side. In the first case, the server itself, before transmitting a web page, examines the HTML code and replaces in real time some markers by data, which can be, for instance, the result of a call to a SQL server. It is the way in which the well-known MySQL/PHP team works.

The transclusion can also be performed in real time by the browser itself. In this case, the browser will seamlessly issue an HTTP request to download content to a web site potentially external to the visited domain (i.e., not belonging to the same domain). By doing so, the browser, while opening an HTTP connection, *can* send

or receive cookies but will *systematically* send the visited webpage URL through the referring page systematically sent in the header of the HTTP request. To be short, external web sites know, while being accessed by transclusive hyperlinks, the complete URL of the web page visited, the individual IP address, the browser brand and the version of the OS[1], etc. As we will detail below, transclusive hyperlink is the technique massively used by cyber marketing companies many billion of times a day since a decade now.

It means that, by default, a cyber marketing company knows in real time all the keywords typed by a particular netizen on a search engine on which he is advertising, the computer, operating system, browser brand of the netizen, the IP address he is using and the time and duration of the HTTP sessions. Those data are called the "clickstream": and permit to infer some supplementary data like[2]

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.

The cookies issues have already been widely discussed. The cookie mechanism was introduced by Netscape in their well-known Navigator in 1996. The SET-COOKIE is invisibly taking place in the HTTP response header and may thus be sent through transclusive hyperlinks. The icing on the cake is called web redirection. Through transclusive hyperlinks, cyber marketing agencies are collecting, on an individual basis, the daily clickstream of the vast majority of netizens. If the cookie feature remains enabled (as it is by default in most widespread browsers like IE, Firefox, Safari and Opera), the traceability of hundreds of millions of users is activated and permit cyber marketing agencies (and to secret services?) to follow each person, notwithstanding changes of IP addresses, for many years.[3]

In Belgium, all the press on line, many social networks, many forums, auctions websites, etc are monitored by Google-Analytics. As a concrete result, the webmaster may benefit from beautiful pie-charts showing their audience. As a concrete result, just because the huge majority of web sites are using the same technology with real time transclusive hyperlinks to the Google website in US, Google can

[1] I did call that browser chattering as far as those data are not necessary to a correct data transmission. The original HTTP specification was foreseeing a field named "from" containing nothing else than the email address of the internet user.

[2] 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

[3] In practice, the cookies are not linked to a particular computer but to a particular user of a computer. That is to say, two different users with their own session on the same computer will use different cookie files.

know, on the individual basis of the IP address, the individual clickstream of netizens among virtually all web sites within and outside Europe.

One may object that the dynamic IP addressing scheme is offering a protection and avoids cross profiling the same individual day after day. Technically speaking, this is not a valuable objection if we do take into account the fact that

- Doubleclick is systematically using a permanent unique identifying cookie
- Doubleclick is present among various web sites and it is almost impossible to surf ten minutes on popular web sites without opening transclusive hyperlinks to DoubleClick
- As a consequence, DoubleClick is able to identify all the dynamic IP addresses used by the same netizen, just because those IP addresses have been sent together with a single unique identifying cookie
- Google bought DoubleClick in May 2007.

5.4 The Ontological Approach

Since about five years, there has been much research funded by the EC related to the ontology of privacy and identity (Fidis, Rapid, Prime, Swami, etc). One tangible output of those researches is the classification built by Andreas Pfitzmann[4], which identifies different levels of privacy (unobservability, untraceability, pseudonymity and anonymity). These concepts may be used on the Internet to gauge the level of privacy of a netizen. From a technical point of view, whenever an intrusive popup window or a spam may be personal data processing or not, is irrelevant as far as intrusive popup windows or spam obviously compromise the availability, the integrity and the confidentiality of the netizen's information system.

European Data Protection legislation (General Data Protection Directive[5] and eDirective[6]) does not, in practice, fill two major gaps in the net of the protection of the privacy. Among the men in the street, there is currently confusion between privacy and data protection. In Europe, legal protection is mainly granted to so-called "personal data[7]", i.e., data related to an identified or identifiable person. This

[4] Andreas Pfitzmann, Marit Köhntopp: Anonymity, Unobservability, and Pseudonymity – A Proposal for Terminology; in: H. Federrath (Ed.): Designing Privacy Enhancing Technologies; Workshop on Design Issues in Anonymity and Unobservability, July 25–26, 2000, Intern. Computer Science Institute (ICSI), Berkeley, CA, LNCS 2009, Springer-Verlag, Heidelberg 2001, 1–9.

[5] 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, OJ L 281, 23.11.1995, p. 31.

[6] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.07.2002, p. 37.

[7] Following Article 2 (a) of Directive 95/46: " 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who

is to say that global surveillance of individual actions such as browsing, consumer's behaviours, receptivity to eMarketing and so on are not, as such, in the "ratio materiae" of European Directives, as long as data collected remain fully anonymous. The anonymous surveillance is not forbidden by the EU data protection legislation even if this kind of surveillance may be contrary to Article 8 of the European Convention of Human Rights.[8] This is not to say that anonymous observations are, legally speaking, systematically allowed. It will certainly not be the case when the surveillance is conducted by using intrusion techniques such as trojan horses, malware, spyware or viruses, or communication tapping in the framework of a "man-in-the-middle" attack. In brief, the right to data protection does not exhaust the right to privacy.

A second lack in the European data protection legislation with respect to the protection of privacy can be found in the notion of "data controller" as laid down by Art . 2 (d) of the general data protection directive. The controller is the natural or legal person, public authority, agency or any other body that alone or jointly with others determines the purposes and means of the processing of personal data.

Both the definition of personal data and the definition of the data controller create two holes in the net in European data protection legislation towards privacy protection. On the first hand, human data not related or linkable to individuals are not subject to the application of the directive. On the second hand, massive human data processing (e.g., invisible processing through implicit hyperlinks to third party (so called "web bugs") and third party identifying cookies) have no data controllers, as far as Bill Gates is not the "data controller" of invisible HTTP connections (involving the sending of cookies and referring pages) seamlessly processed by MSIE, even if, just as underlined by the Recommendation, "those who design technical specifications and those who actually build or implement applications or operating systems bear some responsibility for data protection from a societal and ethical point of view."

In May 2007, the EC Commission issued a communication on promoting Data Protection by Privacy Enhancing Technologies.[9]

After giving a general definition of what can be included in PETS: "appropriate technical measures ..." and underlining that PETS should be "an integral part in any efforts to achieve a sufficient level of privacy[10] protection", four examples of

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;"

[8] See in this direction the recent opinion 4/2007 of the Article 29 data protection working party on the concept of personal data, pp 24: "Where data protection rules does not apply, certain activities may still constitute an inference with Article 8 of the European Convention on Human Rights, which protect the right to private and family life... Other sets of rules, such as torts laws, criminal law or antidiscrimination law may also provide protection to individuals in those cases where data protection rules do not apply and various legitimate interests may be at stake."

[9] Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs) /* COM/2007/0228 final */, Brussels, 2.05.2007.

[10] Fortunately, the target is here to improve the privacy, not the personal data protection.

PETS are given. Those examples include the automatic anonymization, Encryption tools, Cookie-cutters and P3P.

Those examples are problematic because they are neglecting the current state of the art and the fundamental concern of data subjects, whatever the name put on it (privacy, security or data protection).

The encouragement to the anonymization of data may let believe that anonymous surveillance is fully compatible with privacy. The highest level of privacy remains non observation and involves that data related to human beings such as – but not limited to – localization, consumption habits, surfing behaviours, etc., are not recorded at all. This privacy level is detailed as being the first level of privacy and security in the ISO standard 15408. This issue is becoming more and more sensitive, notably due to the wide spreading of RFID's in all our surrounding objects. With regard to a general privacy requirement, routine observation of a growing number of slices of human lives seems not socially acceptable, even if those observations are anonymized as soon as possible.[11]

In the field of encryption, the communication focuses on the prevention against interception during the transmission of information (so-called "man-in-the-middle" attack). Encryption tools like PGP for the electronic mail, SSL for the surf and SSH for file transfer are nowadays widely available and deployed. Those tools are secure enough to resist a brute force attack.

The mention of cookies-cutters appears the most surprising example of some kind of innovative Privacy Enhancing Technologies. In practice, since many years, all modern browsers provide embedded and user-friendly cookie control features. Genuinely, out of the box browsers like MSIE, Firefox, Safari or Opera provide since many years cookie management tools that may inhibit or reduce the permanency of cookies, providing a relevant distinction between cookies sent by the current website and cookies sent by invisible third parties. At the light of those privacy enhancements embedded in the current technology, a cookie-cutter approach under the form of an external program or a plug-in seems today, with respect to the current state of the art, to be widely deprecated.

Perhaps the communication of the European Commission should have been more innovative and efficient by suggesting the total suppression of the cookie mechanism itself. This suppression is not unrealistic, because, from a functional view point, alternative solutions, less privacy killing, exist to fill actual and legitimate proposes of cookies.

Session cookies may very easily be put at the visible URL level (e.g., www.ebay.com?sessionID=ZE34TR) rather than in the invisible HTTP header. This system is widely used by many web servers working with PHP or ASP. For permanent

[11] See also the recent opinion 4/2007 of the Article 29 data protection working party on the concept of personal data P. 24: "Where data protection rules does not apply, certain activities may still constitute an inference with Article 8 of the European Convention on Human Rights, which protect the right to private and family life... Other sets of rules, such as torts laws, criminal law or antidiscrimination law may also provide protection to individuals in those cases where data protection rules do not apply and various legitimate interests may be at stake."

cookies, if they originate from third parties, they will allow following a single user seamlessly (cookies are linked to a user and not to a computer) on an individual basis during his whole click stream (pages of newspaper read, keywords typed on search engines, interventions in discussions forums, etc.) and are clearly putting the privacy of the surfer at risk (confidentiality breach). If the cookie originates from a web site voluntarily visited, it appears to be more efficient to implement a classic system of userID/password that will permit to the user, through a simple and positive action to be identified and profiled, or, on the opposite, to surf the web site anonymously. Here again, all modern browsers are proposing embedded password management systems that are more secured than cookies and that avoid repeated typing of an ID and password to the user (the browser seamlessly recognizes a recent authentication form and automatically proposes the last typed ID and password; at the opposite of the cookie mechanism, the user may not be identified nor tracked without his preliminary and ad hoc consent).

Cookie type	Privacy risk	PET solution
Direct session	None: Traceability risk not higher than that of a dynamic IP address	Put the cookie in the URL www.ebay.com?sessionID= ZE34TR rather than in the invisible HTTP header
Direct remanent	Important: Unfair and invisible identification and trackability	Use of ID/password Management systems already embedded in all modern browsers
Third party (session or remanent) = Transclusive hyperlink	Very High: Unfair, routine and invisible trackability by a foreign, invisible and untrusted third party	Must be forbidden

A browser without any cookie capability – this should have been a realistic and popular privacy enhanced requirement.

In the P3P field, following a survey performed by SecuritySpace[12], P3P policy deployment ratios have evolved between 1 and 5% of web sites ranked since the P3P's launching in 2002. It has to be noticed that Opera, Safari and Firefox does not support P3P, this means that Apple, Linux and Unix users are out of the game. The single reference implementation of P3P lies in MSIE on MS-Windows and permits, by default, to cyber marketing (like DoubleClick) and audience measurement companies to put an identifying permanent cookie on the workstations of millions of naïve netizens (for the purpose of tracking them through the referring page systematically sent by common browsers). In practice, it is sufficient for a marketing company to establish a compact privacy policy aiming that no personally identifiable information is collected or stored to pass through the P3P default settings of MSIE. P3P was deeply criticized many years ago both by the Article 29 working

[12] http://www.securityspace.com/s_survey/data/man.200706/p3p.html

party[13] and by the International Working Party on the Protection of Individuals[14] in these terms: "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". The Electronic Privacy Information Center speaks about a Pretty Poor Privacy.[15]

Data subjects may regret that, in this enumeration of examples, the issues of Global Unique Identifier (like the MAC address in Ipv6 addresses or serial number of RFID chips) or transclusive hyperlinks (web bugs) to untrusted third parties have not been considered.

5.5 When Non DP Laws Help to Fill the Gaps in Existing Data Protection Legislation to Enhance Privacy Protection

The objectives described in the Communication are (1) to support the development of PETs, (2) to support the use of PETs by data controllers and (3) to encourage consumer's to use PETs.

Within the first objective, the Communication proposes to identify the need and the technological requirements of PETs and plans to call national authorities and the private sector to invest in the development of PETs. It has to be underlined that the focus here is not the protection of personal data but to provide "the foundation for user-empowering privacy protection".

In the framework of the second objective, the Communication aims to promote the use of PETs by industry and to ensure the respect for appropriate standards in the protection of personal data through the standardisation and the coordination of national technical rules on security measures for data processing. Very surprisingly, the Recommendation does not mention ISO and notably the recent standard ISO 15408. Finally, the Communication wants to involves public authorities, promoting their use of PETs.

The last objective is to encourage consumers to use PETs by raising their awareness and develop an EU-wide system of privacy seals.

At the lecture of these objectives, I got the feeling that the Communication may perhaps be a mix between the objectives of PETs and the means to reach the objectives. Furthermore, the wide spreading of PETs is not an objective in itself but rather a means to enhance the privacy of human beings through Europe, without having to pay the price of negotiating the immutable value of privacy to obtain a user-friendly information society.

[13] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1998/wp12_en.pdf
[14] http://www.datenschutz-berlin.de/doc/eu/gruppe29/wp11_en.htm
[15] http://www.epic.org/reports/prettypoorprivacy.html

Before creating new Privacy Enhancing Technologies, it appears evident that it is more effective to routinely produce information technologies that are privacy keeping, by default.

In the field of the mobile phone, we have reached a very good balance between privacy and surveillance. The consumer can benefit from the Calling Identification Line Indication that permits to identify the number of the mobile calling; at the same time the same consumer can benefit from the Calling Line Identification Restriction that allows him to hide his own number when calling somebody. For security reasons, emergency services can know, whatever the CLIR status can be the calling number of the emergency service caller. Just because the calling number is technically transmitted by the telecom operator, the transmission of a false phone number is quite impossible. The communication is fully encrypted by a 40 bit key and a man-in-the-middle attack appears to be very difficult. Each phone has a unique identifier (IMEI) but this identifier is sent to the telecom operator who does not relay it to the called person's terminal. This high level of privacy has been reached also because there has been a long tradition of privacy in the telecommunication world. But to me, a relevant cause of this success story is the fact that a mandatory telecommunication agreement (including privacy consideration) was necessary before putting a mobile phone device on the market.

In the field of electronic mail, a netizen may very easily change his sender address (what spammers do a billion times a day) just because the email address is sent by the email program and not by the network operator. If a netizen is using Ipv6 configured by default in MS-Windows workstations, the recipient of an email may track the same netizen even if (s)he is using different legitimate "anonymous" email addresses just because the Ipv6 address incorporates by default the serial number of the network interface card of the PC ("Mac Address").

In the field of the Internet, it may be relevant to have a glance at recent history. The technological move originated in the very beginning from the Personal Computers appearing at the beginning of the eighties. Local Area Network (LAN) started to appear in the mid-eighties and the World Wide Web started in the early 90s. The cookies mechanism itself was specified by Netscape in 1996, without any reference to the newly born Directive 95/46.

Now the Internet is present everywhere, but telecommunication terminals[16] (not limited to hardware but including software and firmware) are not privacy compliant, more precisely, software like browsers are not "incorporating [sufficient] safeguards to ensure that the personal data and privacy of the user and the subscriber are

[16] In the wide meaning of Directive 99/5 of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity in Article 2 (b): *(b)* "'telecommunications terminal equipment' means a product enabling communication or a relevant component thereof which is intended to be connected directly or indirectly by any means whatsoever to interfaces of public telecommunications networks (that is to say, telecommunications networks used wholly or partly for the provision of publicly available telecommunications services)."

protected" (one of the essential requirements foreseen in Article 3.3.c of Directive 99/5).

It has to be noticed that such privacy specifications have already existed for many years. For instance, the word "privacy" appears 28 times in the RFC defining the HTTP protocol. But, insofar as they appear in the form of recommendations ("should") the ITC industry did not implement them into software like browsers. Concerning the incorporation of the Mac Address in Ipv6 addresses, privacy compliant alternatives like the "Privacy Extensions for Stateless Address Autoconfiguration in Ipv6", a RFC issued by the well-known IETF.

Last but not least, it may appear very surprising that the Communication – issued by the Commission – does not take on board existing legal tools that permit the European Commission itself to enforce privacy regulation by the ICT industry. Notably Article 5.2 of Directive 99.5, which states "Where a Member State or the Commission considers that conformity with a harmonised standard does not ensure compliance with the essential requirements referred to in Article 3, which the said standard is intended to cover, the Commission or the Member State concerned shall bring the matter before the committee" or Article 15 of Directive 2002/58 that states "2. Where provisions of this Directive can be implemented only by requiring specific technical features in electronic communications networks, Member States shall inform the Commission . . .3. Where required, measures may be adopted to ensure that terminal equipment is constructed in a way that is compatible with the right of users to protect and control the use of their personal data, in accordance with Directive 1999/5/EC . . ."

Will Europe, finally, take the opportunity to put into the prestigious "CE" label stamped on telecommunication hardware and software some substantive, innovative and mandatory requirements for a European Privacy Compliant Technology?