Privacy Challenges in Marketing Practices
European (over)ruling of the use of personal data? [1]

By Avv. Felix Hofer [23]

1. In order to promote their products and services effectively marketers need extensive information about the subjects they're dealing with or they'd like to target for future business. Technical progress requires such information to be more and more sophisticated: in order to perform a successful campaign it's crucial to know as much as possible and in detail about targeted companies, individuals, categories, industry sectors, shopping habits, consumer profiles, gender, race, age, location, financial capacity and health conditions.

That's the reason why nowadays 'data' has become the most valuable 'raw material' in the modern economy. That is also the reason why marketers' techniques for approaching target subjects have become extremely complex and rely on top level technology.

Marketers' business nowadays involves practices such as behavioral-, contextual-, location- and mobile marketing; it extends way beyond (earlier) traditional media, reaching out to the on-line communities (virtual worlds, social networks, blogs, discussion forums, etc.) and makes use of advanced technological tools – especially in the area of neuromarketing - such as Radio Frequency Identification (RFID), Functional Magnetic Resonance Imaging (fMRI), Steady State Topography (SST), Facial Coding and Galvanic Skin Response[4]. And yes, cookies are still immensely popular and widely used.

2. Practices that dwell so deep into an individual's personal sphere, do monitor his habits and profile many aspects of his personality, are also capable to cause data subject's annoyance and opposition.

More and more frequently we find reports in the news – both in Europe as well as in other geographic regions around the world - about clashes between aggressive marketing techniques and privacy concerns. Nevertheless I feel that the exact dimension and the real terms of this problem are still not correctly perceived. Any time I mention this issue among my colleagues and friends in the US, I face a rather annoyed reaction, usually accompanied by the objection that the 'sacrifice' of giving up a bit of privacy is largely compensated by the multiple benefits one receives from allowing the processing of personal data. When I try to insist and to make my point, my interlocutor generally labels me as 'one of those consumer protection advocates'.

This personal experience is an illuminating example of a patent misperception of a problem, which – if not correctly assessed - could put marketers into serious trouble.

---

1 This paper was prepared as a handout to the audience the Advertising Law & Public Policy Conference 2011 organized by the Association of National Advertisers - ANA in Washington DC, on March 15th & 16th, 2011.

2 ***Felix Hofer*** is a named and founding partner of the Italian law firm Studio Legale Associato Hofer Lösch Torricelli, in Firenze (50132), via Giambologna 2/rosso; he may be reached through the following contact details: Phone +39.055.5535166, Fax +39.055.578230 – e-mail: fhofer@hltlaw.it (personal) or info@hltlaw.it (firm e-mail).

3 Member for Italy of the Global Advertising Lawyers Alliance (GALA), www.gala-marketlaw.com

4 To tell it right, most of the technology has been around and tested for decades; what's changed is their use in the area of marketing and the quality both, of the technical devices as well as of the software applications used to the purpose.

3. First of all, foreign companies not familiar with the European approach to processing of personal data and with the laws and regulations governing such practice need to realize that on this side of the Atlantic 'privacy' has little to do with consumer protection: the issue at stake (and the interest considered by legislation) is not that of avoiding "harm" to consumers, but that of granting individuals a **fundamental right**, which benefits from protection at a maximum (i. e. constitutional) level.

The Charter of Fundamental Rights of the European Union[5] clearly states (in Article 8 on 'Protection of personal data') that *"1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority"*.

Well ahead of the Treaty of Lisbon many countries, members to the European Union, had in their national Constitutions identical or similar provisions, meant to assure adequate protection to an individual's private sphere[6]. The reasons for such an approach are to be found in the historical context surrounding World Wars I and II. In other terms, the 'fundamental right reference' puts the guarantees for an individual's personal data in the same league as freedom of speech and First Amendment protection. Therefore no surprise that infringement of some of the most relevant provisions governing the processing of personal data are sanctioned not just by fines, but also under criminal law.

Any time marketers processing personal information do not give adequate consideration to this aspect and its implications, they may easily find themselves exposed to critical situations and to significant risks for their business practices.

There are a few things marketers ought to bear in mind when crossing the Ocean and addressing the EU's plus 550 million consumers market. Without pretending to result exhaustive and just focusing on the very basic aspects the following comments try to summarize some of the most significant legal implications for companies doing business on an international level.

4. The starting point for a correct privacy policy are clearly the principles laid down in the so-called 'Data Protection Directive' [7]. While recognizing the importance of data-processing systems and of data-flow without excessive obstacles, these principles also claim that handling of an individuals' personal information has to *"respect their fundamental rights and freedoms, notably the right to privacy"*.

Accordingly the Directive requires[8] all personal data to be:

- processed fairly and lawfully,
- collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes,
- adequate, relevant and not excessive in relation to the purposes for which they are collected,
- accurate and, where necessary, kept up to date,
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected, and

establishes[9] that personal data may be processed legitimately only if the data subject has unambiguously given his consent, or processing is necessary:

- for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract, or
- for compliance with a legal obligation to which the controller is subject, or

---

5 In its current version the Treaty of Lisbon entered into force on 1 December 2009.

6 The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data signed on January 28th, 1981 in Strasbourg by the member States of the Council of Europe already anticipated - and addressed – some of the issues currently in discussion.

7 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995.

8 See Section no. 6/1 of the Directive.

9 See Section no. 7 of the Directive.

- in order to protect the vital interests of the data subject, or
- for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed, or
- for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1.

5. This initial framework was then completed by the *ePrivacy* Directive[10] (amended and integrated in year 2009[11]), which extends the requirements set by the '95 Directive to *"publicly available electronic communications services in public communications networks"*. This additional Directive clarifies that *"Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms"* [12] and enlightens about the limits of legitimate use of cookies[13]. Finally, it gives indications as to the collection, use and storage both of 'traffic data' as well as of 'location data' [14] and provides for measures specifically aimed at granting data security and confidentiality of communications[15].

Under the provisions of this Directive companies making use of cookies were held to: (a) provide targeted subjects with clear in-advance indications about the installation of cookies on user's terminal as well as about their function and purposes, (b) achieve users' consent for placing cookies, and (c) inform them about their possibility to refuse cookies' placement on their terminal and about the browser settings apt to exercise such blocking right[16].

6. This earlier 'notice and choice' regime for the use of cookies is now subject to changes introduced by the so-called 'cookie' Directive[17], which is due to be implemented by the EU member states no later than by May 25th, 2011.

---

10 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).

11 Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009.

12 So Recital 24 of the Premises of Directive no. 58 of 2002, where it's also stated that *"So-called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users. The use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned"*.

13 According to Recital 25 *"... such devices, for instance so-called 'cookies', can be a legitimate and useful tool, for example, in analysing the effectiveness of website design and advertising, and in verifying the identity of users engaged in on-line transactions. Where such devices, for instance cookies, are intended for a legitimate purpose, such as to facilitate the provision of information society services, their use should be allowed on condition that users are provided with clear and precise information in accordance with Directive 95/46/EC about the purposes of cookies or similar devices so as to ensure that users are made aware of information being placed on the terminal equipment they are using. Users should have the opportunity to refuse to have a cookie or similar device stored on their terminal equipment. This is particularly important where users other than the original user have access to the terminal equipment and thereby to any data containing privacy-sensitive information stored on such equipment. Information and the right to refuse may be offered once for the use of various devices to be installed on the user's terminal equipment during the same connection and also covering any further use that may be made of those devices during subsequent connections. The methods for giving information, offering a right to refuse or requesting consent should be made as user-friendly as possible. Access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose"*.

14 See Sections nos. 6 and 9 of Directive no. 58 of 2002.

15 See Sections nos. 4 and 5 of Directive no. 58 of 2002.

16 Section 5/3 of the ePrivacy Directive no. 58 of 2002 rules that *"Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user."*

17 Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector.

The amending provisions contain several rather challenging principles and recommendations to providers as well as binding provisions apt to significantly affect marketing practices.

As to the first aspect the amending Directive no. 136 of 2009:

- claims for proper notice to customers with respect to their rights concerning information contained in subscriber directories (and the purposes of such directories) and for adequate measures in order to safeguard the personal information of (fixed and mobile) end users collected in databases[18],
- reminds that 'traffic data', if "controlled" by providers of security technologies and services, are subject to the requirements of Directive no. 46 of 1995[19] ,
- while acknowledging the importance and the unquestionable benefits of *"new applications based on devices for data collection and identification"* such as Radio Frequency Identification Devices, requires that their use has to result 'acceptable' to the targeted individuals and must ensure individual's fundamental rights, inclusive that to privacy and data protection[20],
- insists [21]on the fact that all providers of publicly available electronic communications services should immediately report any data breach they become aware of and notify without delay all subscribers and individuals adversely affected by such breach,
- alerts[22] about the risks involved by the use of *"software surreptitiously monitoring actions of the user or subverting the operation of the user's terminal equipment to the benefit of a third party (spyware)"* and therefore calls for a *"a high and equal level of protection of the private sphere of users … to be ensured, regardless of whether unwanted spying programmes or viruses are inadvertently downloaded via electronic communications networks or are delivered and installed in software distributed on other external data storage media, such as CDs, CD-ROMs or USB keys"*,
- informs third parties wishing *".. to store information on the equipment of a user, or to gain access to information already stored, for a number of purposes, ranging from the legitimate (such as certain types of cookies) to those involving unwarranted intrusion into the private sphere (such as spyware or viruses)"* that they need to provide users *".. with clear and comprehensive information when engaging in any activity which could result in such storage or gaining of access"* [23], and finally
- feels[24] that *"safeguards provided for subscribers against intrusion into their privacy by unsolicited communications for direct marketing purposes by means of electronic mail should also be applicable to SMS, MMS and other kinds of similar applications"*,

As to the binding provisions the most worrying aspect appears to be the "opt-in" mechanism apparently contained in the amended version of Section 5/3[25] of the previous Directive no. 58 of 2002. The new wording seems to present marketers with a true nightmare scenario: under the earlier version of the

---

18 So Recitals nos. 33 and 38. According to Recital 59 all data controllers should implement ".. *appropriate technical and organisational protection measures against, for example, loss of data*".

19 Implying an obligation of "*preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems"* (Recital 53).

20 Additionally, *"when such devices are connected to publicly available electronic communications networks or make use of electronic communications services as a basic infrastructure, the relevant provisions of Directive 2002/58/EC (Directive on privacy and electronic communications), including those on security, traffic and location data and on confidentiality, should apply"* (Recital 56).

21 See Recital 61.

22 So Recital 65

23 See Recital 66, also recommending that "*The methods of providing information and offering the right to refuse should be as user-friendly as possible. Exceptions to the obligation to provide information and offer the right to refuse should be limited to those situations where the technical storage or access is strictly necessary for the legitimate purpose of enabling the use of a specific service explicitly requested by the subscriber or user. Where it is technically possible and effective, in accordance with the relevant provisions of Directive 95/46/EC, the user's consent to processing may be expressed by using the appropriate settings of a browser or other application"*.

24 So Recital 67.

25 *Article 5(3) shall be replaced by the following: "3. Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service."*

Directive it was possible to place a cookie and then to seek for consent, according to a strict reading of the amended text now placement of a cookie should be allowed only after having obtained targeted subject's (informed) in-advance consent[26].

The only exception to this general rule would be permitted when storage of (or access to) personal information:

(a) is performed exclusively in order to carry out the transmission of a communication over an electronic communications network; or

(b) results necessary for providing an information society service specifically requested by the subscriber or user.

It goes without saying that a strictly opt-in oriented requirement for placing cookies would determine simply "devastating" effects not just for the marketing industry, but to websites in general (commercial and non-commercial ones), almost all relying on (and making use of) cookies.

7. With respect to data processing the direct marketing industry needs to consider also some additional aspects.

7.1. Already back in year 2008 the Article 29 Working Party [27] had reminded [28] Internet companies operating search engines that in its view the provisions of the Data Protection Directive no. 46 of 1995 did *"apply to the processing of personal data by search engine providers in many cases, even when their headquarters are outside the EEA"* and that multinational search engine providers were subject to the national laws governing the handling of personal information (aside from the case where they had an 'establishment' in a country member to the EU), when a *"company makes use of equipment, automated or otherwise on the territory of that Member State, for the purposes of processing personal data (for example, the use of a cookie)"* [29]. A further confirmation of the Working Party's position may be found in Opinion 1/2009 [30] informing search engines, once more, about its convincement that:

- *"beyond all doubt that the processing of traffic data falls within the scope of the Data Protection Directive"*,
- unless a service provider *"is in a position to distinguish with absolute certainty that the data correspond to users that cannot be identified, it will have to treat all IP information as personal data, to be on the safe side"* (reference is to *"additional identifiers such as cookies"*).

7.2. A few month later the Working Party, while offering its contribution[31] to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, took the view that *"The technological developments have strengthened the risks for individuals' privacy and data protection and to counterbalance these risks, the principle of 'Privacy by Design' should be introduced in the new framework: privacy and data protection should be integrated into the design of Information and Communication Technologies"* [32] and claimed that privacy should 'become embedded in ICT', while additionally stressing

---

26 Where 'informed consent' means that users have also to be provided with comprehensive and easy to understand information about all the purposes which collected data will be processed for. Subsequently, if a purpose changes for whatever reason, an additional consent will have to be sought.

27 An independent EU Advisory Body (set up by Directive 95/46/EC) for providing expert opinion from member state level to the EU Commission on questions of data protection, promoting harmonized application of the general principles of the Directives in all Member States through co-operation between data protection supervisory authorities, advising the EU Commission on any Community measures affecting the rights and freedoms of natural persons with regard to the processing of personal data and privacy.

28 So Opinion 1/2008 – WP 148 - on data protection issues related to search engines adopted on April 4th, 2008.

29 In previous Opinion 4/2007 - WP 136 - of 20th June 2007 (on the concept of 'personal data') it had already made clear that an individual's search history, IP addresses and cookies had to be considered as "*data relating to an identifiable person*" any time identification is possible by relying on reasonable means likely to be used.

30 WP 159, issued on February 10th, 2009 with respect to the draft text of Directive no. 136/2009.

31 WP 168 of December 1st, 2009.

32 Where "*the application of such principle would emphasize the need to implement privacy enhancing technologies (PETs), 'privacy by default' settings and the necessary tools to enable users to better protect their personal data (e.g., access controls, encryption). It should be a crucial requirement for products and services provided to third parties and individual customers (e g. WiFi-Routers, social networks and search engines). In turn, it would give DPAs more powers to enforce the effective implementation of such measures*" (see page 13, point no. 48).

that *"Under the Lisbon Treaty, data protection has gained significant importance. Not only has the Charter of Fundamental Rights of the European Union become binding but – also Article 16 of the Treaty on the Functioning of the European Union (TFEU) was introduced as a new legal basis for data protection applicable to all processing of personal data, in the private and in the public sector, including the processing in the area of police and judicial cooperation and common foreign and security policy"*.

7.3. In year 2009 social networks have also come under the Working Party's scrutiny. In an Opinion [33] dedicated to sector specific problems the Working Party offered its comments (and guidelines) on how and to which extent social networks are affected by the principles laid down in the Data Protection Directives, on which requirements and obligations social networks are held to comply with[34] and on which user rights have to be adequately granted by the platform providers[35]. A special section of the WP's opinion is dedicated to direct marketing[36], recognized as *"an essential part of the SNS business model"*, but also required to *"comply with relevant provisions of both Data Protection and ePrivacy Directive"*.

7.4. To round off the issue it should be mentioned that back in 2010 the Working Party had issued an extensive Opinion[37] on the topic of online behavioral advertising (resulting in user tracking mechanisms and profile construction[38]) and its privacy implications. While the paper does not question the multiple advantages and economic benefits offered by such practice, it does flag serious concern about the possibility of such practice being performed *"at the expense of individual's rights to privacy and protection of personal data"*.

In order to provide harmonized guidance to network providers making use of behavioral targeting the Opinion offers a number of indications, according to which:

- both, placing of cookies or similar devices on users' terminal equipment as well as obtaining information through such devices may legitimately occur only on 'user's informed consent',
- current browser settings and op-out systems may not adequately fulfill such consent requirement (especially when bypassing users' choice is possible),
- network providers should put in place proper in-advance opt-in mechanism *"requiring an affirmative action by the subjects indicating their willingness to receive cookies and similar devices and the subsequent monitoring of their surfing behavior for the purpose of serving tailored advertising"*,
- consent to cookie placement may imply users' acceptance of its reading and of the monitoring their browsing habits,
- for keeping users' aware about monitoring being performed providers should: *"(i) limit in time the scope of consent, (ii) offer the possibility of revoke it easily, and (iii) create visible tools where the monitoring takes place"* [39].

On the premise that behavioral advertising implies the use of 'identifiers' capable of elaborating *"very detailed user profiles, which in most cases will be deemed personal data",* the Working Party:

- reminds providers that profiles achieved may easily result subject to the provisions of the Data Protection Directive no. 95/46 and specifically to those relating to adequate in-advance notice about

---

33 Opinion 5/2009 – WP 163 - on on-line social networking, adopted on 12 June 2009.

34 E. g. as to indications about providers' identity, information about purposes and ways of data uses, warnings about privacy risks related to data posting, availability of privacy-friendly default settings, copyright and minors' protection, respect of other data subjects' rights, handling of abandoned accounts.

35 Among them inclusive an easy-to-use complaint handling procedure and user's possibility of adopting pseudonyms.

36 Section 3.7, which addresses contextual, segmented and behavioral marketing. I restrain from reporting extensively on the legal issues referring to social networks as this was dealt with in a paper prepared for the ANA Advertising Law & Public Policy Conference 2010; the paper is available on my law firm's website (at the URL: www.hltlaw.it), in the "News" Section.

37 Opinion 2/2010 - WP 171 – adopted on June 22nd, 2010.

38 The Working Party describing such practices offers the following as its definition of 'profiling mechanism': "*Whereas contextual advertising and segmented advertising use 'snap shots' of what data subjects view or do on a particular web site or known characteristics of the users, behavioural advertising potentially gives advertisers a very detailed picture of a data subject's online life, with many of the websites and specific pages they have viewed, how long they viewed certain articles or items, in which order, etc.*", see Introduction, Section no. 2 of the Opinion no. 2/2010.

39 See Executive Summary on page 3 of Opinion no. 2/2010.

processing purposes, access to and rectification, erasure and retention of data,
- takes the position that, given the nature and characteristics of such practice, it's essential to targeted individuals having adequate transparency requirements granted[40]

7.5. The fact that the European Data Protection Supervisor[41] has addressed all the aspects mentioned above on several occasions clearly shows how intense the focus of the EU Institutions is on privacy implications.

In a speech delivered at Future Internet Assembly[42] the EDPS highlighted the *"privacy implications of ICT and new services: social networks, search engines, RFID tags, browsers, targeted advertising, cloud computing.."* and voiced his concern about potential negative structural effects likely to be derived – if not timely and properly addressed – in the context of *".. more complex environments, such as the collection of data through Internet, mobile devices, RFID, etc"* [43].

8. To conclude this excursus on privacy regulations in Europe a few comments on some critical aspects foreign companies should bear in mind when directing their business and promotional strategies towards Europe.

8.1. Up till now in the context of the discussion about the opt-in requirement for cookies it seems to have gone somehow unnoticed that the new text of Section 5/3 of the ePrivacy Directive[44] refers to 'information' about users, which is clearly a different – and much broader - definition than that of 'personal data'. Section 5/3 therefore seems to result in a sort of 'general provision' meant to cover (and protect) an area of users' private sphere extending beyond the context of the rights and guarantees typically reserved to an individual's personal data.

8.2. There is an additional aspect which deserves proper attention: user monitoring and profiling essentially do originate from information collected by placing cookies or similar devices on an end-users' terminal. This means that 'processing' of data is performed (at least partially) in the place where user's technical equipment is located. From such premise derive necessarily several interesting – and highly worrying – effects and consequences as to jurisdiction and applicable law.

8.3. Advertisers usually display their commercial campaigns on their own websites and have mechanisms in place allowing click-through analysis. Based on elaborating information about surfing behavior, they then frequently perform in 'profiling' and determining interest groups, segments or sector specific information (those fond of country music, teenagers aged between X and Y loving a certain product or service, minors being already parents of children, etc.). Under European privacy regulations advertisers, by elaborating and categorizing information in such a way, easily may found themselves considered as 'data controllers' (as such subject to a range of provisions contained in the EU Directive no. 95/46). They'll be better off by knowing exactly which requirements and prescriptions they should comply with, especially when profiling results on 'categorizing' with respect to sensitive personal data.
Network providers or online publishers will also be held as 'data controllers' any time they perform in elaborating on their platforms the personal information collected from third parties.

---

40 The Working Party makes the assumption that *"in the context of behavioural advertising users may not know or understand the technology that supports behavioural advertising or even that such types of advertising are being targeted at them"* and therefore holds that *"it is therefore of paramount importance to ensure that sufficient and effective information is provided in a way that will reach internet users. Only if data subjects are informed, will they be in a position to exercise their choices"* (so Opinion no. 2/2010, page 17, Section 4.2.

41 The EDPS is an independent supervisory authority devoted to protecting personal data and privacy and promoting good practice in the EU institutions and bodies. It does so by: monitoring the EU administration's processing of personal data, advising on policies and legislation that affect privacy, and co-operating with similar authorities to ensure consistent data protection.

42 In Ghent, on December 16th, 2010.

43 The views of the EDPS are also explained in a recent article *"Data protection in the information society"*, authored by the Chair of the Institution, Mr. Peter J. Hustinx, and published in the collection "Massificatie in het privaatrecht", Essays marking the bicentenary of the society Iustitia et Amicitia, Deventer, 2010, pp. 77-91. In addition I'd suggest checking the Opinion issued by the EDPS on January 14th, 2011. All documents may be accessed on the EDPS website at the URL: http://www.edps.europa.eu/EDPSWEB/.

44 Directive no. 58 of 2002, as amended by Directive no. 136 of 2009.

8.4. One should also bear in mind that the EU Directive no. 95/46 establishes a basic principle according to which personal data legitimately collected for certain purposes may not destined to ‘secondary uses’. Ad networks typically tend to perform multiple services among companies part to the group. In addition, frequently such networks come up with new services or application for which information collected in the context of behavioral advertising is immensely valuable. Unfortunately, in most cases sharing such information – and integrating and adapting it – for new services or application without fulfillment of the in-advance notice and consent requirements will result in an illicit practice.
The same goes for excessive data storage: data retention over the period and the purposes covered by the initial (legitimate) collection is not allowed.

(Reference date: March, 2011)