ARTICLE 29 DATA PROTECTION WORKING PARTY

00909/10/EN
WP 171

Opinion 2/2010 on online behavioural advertising

Adopted on 22 June 2010

Table of Contents

Executive Summary

Behavioural advertising entails the tracking of users when they surf the Internet and the building of profiles over time, which are later used to provide them with advertising matching their interests. While the Article 29 Working Party does not question the economic benefits that behavioural advertising may bring for stakeholders, it firmly believes that such practice must not be carried out at the expense of individuals' rights to privacy and data protection. The EU data protection regulatory framework setting forth specific safeguards must be respected. To facilitate and encourage compliance, the present Opinion clarifies the legal framework applicable to those engaged in behavioural advertising.

In particular, the Opinion notes that advertising network providers are bound by Article 5(3) of the ePrivacy Directive pursuant to which placing cookies or similar devices on users' terminal equipment or obtaining information through such devices is only allowed with the informed consent of the users. The Opinion notes that settings of currently available browsers and opt-out mechanisms only deliver consent in very limited circumstances. The Opinion asks advertising network providers to create prior opt-in mechanisms requiring an affirmative action by the data subjects indicating their willingness to receive cookies or similar devices and the subsequent monitoring of their surfing behaviour for the purposes of serving tailored advertising. The Opinion considers that users' single acceptance to receive a cookie may also entail their acceptance for the subsequent readings of the cookie, and hence for the monitoring of their internet browsing. Thus, to meet the requirements of Article 5(3) it would not be necessary to request consent for each reading of the cookie. However, to keep data subjects aware of the monitoring, ad network providers should: i) limit in time the scope of the consent; ii) offer the possibility to revoke it easily and iii), create visible tools to be displayed where the monitoring takes place. This approach would address the problem of burdening users with numerous notices while ensuring that the sending of cookies and the subsequent monitoring of Internet surfing behaviour for the purposes of serving tailored advertising only takes place with data subjects' informed consent.

Because behavioural advertising is based on the use of identifiers that enable the creation of very detailed user profiles which, in most cases, will be deemed personal data, Directive 95/46/EC is also applicable. The Opinion comments on how advertising network providers should comply with the obligations that arise from this Directive, notably, with respect to rights of access, rectification, erasure, retention, etc. Taking into account that publishers may share certain responsibility for the data processing that takes place in the context of behavioural advertising, the Opinion calls upon publishers to share with ad network providers the responsibility for providing information to individuals and encourages creativity and innovation in this area. Given the nature of the practice of behavioural advertising, transparency requirements are a key condition for individuals to be able to consent to the collection and processing of their personal data and exercise effective choice. The Opinion sets out the information obligations of advertising network providers/publishers vis-à-vis data subjects, referring in particular to the ePrivacy Directive, which requires that users be provided with "clear and comprehensive information".

The Opinion analyses and clarifies the obligations set forth by the applicable legal framework. However, it does not prescribe how, from a technology point of view, such obligations must be complied with. Instead, in different areas, the Opinion invites industry to undertake a dialogue with the Article 29 Working Party with the view to put forward technical and other means to comply with the framework as described in the Opinion as soon as possible. Towards this end, the Article 29 Working Party will contact stakeholders to request their input. Entities that are not explicitly consulted are welcomed to send their contributions to the Secretariat of the Article 29 Working Party.

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995[1],
having regard to Articles 29 and 30 paragraphs 1 (a) and 3 of that Directive, and Article 15 paragraph 3 of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002
having regard to Article 255 of the EC Treaty and to Regulation (EC) no 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents having regard to its Rules of Procedure

HAS ADOPTED THE PRESENT DOCUMENT:

1. Introduction

Online advertising is a key source of income for a wide range of online services and is an important factor in the growth and expansion of the internet economy. However, the specific practice of behavioural advertising raises important data protection and privacy related concerns. Basic internet technology allows advertising network providers to track data subjects across different websites and over time. Information gathered on the surfing behaviour of data subjects is analysed in order to build extensive profiles about data subjects' interests. Such profiles can be used to provide data subjects with tailored advertising.

Given the increasing use of behavioural advertising based on the use of tracking cookies and similar devices and its high level of intrusiveness into people's privacy, the Article 29 Working Party has decided to focus this Opinion on online behavioural advertising across several websites, without prejudice to future opinions, which may analyse other advertising technologies.

With this Opinion, the Article 29 Working Party wishes to clarify the legal framework applicable to those engaged in behavioural advertising. It also invites industry to suggest technical and other means to comply with the framework as described herein as soon as possible and to undertake a dialogue with the Article 29 Working Party regarding such means. Ultimately, the Article 29 Working Party will evaluate the situation and take any measures necessary and appropriate to ensure compliance with the framework set forth herein.

2. Online behavioural advertising

Interactive media advertising refers to a broad range of methods that aim to create more relevant advertisements. The methods may be classified in several categories including contextual advertising, segmented advertising and behavioural advertising.

Behavioural advertising is advertising that is based on the observation of the behaviour of individuals over time. Behavioural advertising seeks to study the characteristics of this behaviour through their actions (repeated site visits, interactions, keywords, online content production, etc.) in order to develop a specific profile and thus provide data subjects with advertisements tailored to match their inferred interests.

[1] Official Journal no. L281 of 23/11/1995, p. 31,

Whereas contextual advertising[2] and segmented advertising[3] 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.

2.1. Ad distribution systems to deliver behavioural advertising

Behavioural advertising involves the following roles: *(a) Advertising networks providers (also referred to as "ad network providers")*, the most important distributors of behavioural advertising since they connect publishers with advertisers*; (b) Advertisers* who want to promote a product or service to a specific audience; and (c) *Publishers* who are the website owners looking for revenues by selling space to display ads on their website(s)[4].

The delivery of ads through advertising networks basically works as follows: the publisher reserves visual space on its website to display an ad and relinquishes the rest of the advertising process to one or more advertising network providers. The ad network providers are responsible for distributing advertisements to publishers with the maximum effect possible. The ad network providers control the targeting technology and associated databases. The larger the advertising network, the more resources it has to monitor users and "track" their behaviour[5]. The advertiser typically negotiates with one or more ad networks and will not necessarily know the identity of all publishers (if any) that will distribute its ads. At the same time, a publisher may have several contracts with different advertising networks, for example by reserving different places on the website for different advertising networks.

There is a growing practice between advertising networks to collaborate with each other through a bidding system[6].

---

2. Contextual advertising is advertising that is selected based on the content currently being viewed by the data subject. In the case of a search engine, content may be derived from the search keywords, the previous search query or the user's IP address if it indicates their likely geographical location.

3 Advertising selected based on known characteristics of the data subject (age, sex, location, etc.), which the data subject has provided at the sign up or registration stage.

4 In addition to advertising networks, behavioural advertising might also be delivered though onsite advertisement. With this method, the advertiser indicates to the publisher its intended audience target based on criteria that may go beyond demographic information such as the traditional triplet of "age range, gender, and country" to much more precise criteria (such as keywords or interests). The publisher then takes care of displaying the advertisement to the chosen target, implementing the targeting technology and controlling the ad placement and distribution. This is used in some social network platforms allowing users to be targeted through their interests.

5 New York Times, "*To Aim Ads, Web is Keeping Closer Eye on You*", 10 March 2008. The article provides statistics about the frequency with which large advertising networks track individual website visits. In case of the Yahoo! advertising network, an average (USA) user was supposedly tracked 2.520 times per month at the end of 2007.
http://www.nytimes.com/2008/03/10/technology/10privacy.html?_r=1&scp=3&sq=%22They%20know%20more%20than%20you%20think%22&st=cse

6 Most major ad networks have a structural collaboration with many other, secondary networks. For example: list of partners for Google Adsense,
URL:http://www.google.com/support/adsense/bin/answer.py?answer=94149,
list of partners for Yahoo!,
URL:http://info.yahoo.com/privacy/us/yahoo/thirdparties/ This works along the following lines: the primary ad network puts the webserver ad space for bidding between several ad networks and picks the best offer.

2.2. Tracking technologies

Most tracking and advertising technologies used to deliver behavioural advertising use some form of client-side processing. It uses information from the user's browser and terminal equipment. In particular, the main tracking technology used to monitor users on the Internet is based on "tracking cookies". Cookies provide a means to track user browsing over an extensive period of time and theoretically over different domains[7].

It usually works as follows: typically, the ad network provider places a tracking cookie on the data subject's' terminal equipment[8], when he/she first accesses a website serving an ad of its network. The cookie is a short alphanumeric text which is stored (and later retrieved) on the data subject's terminal equipment by a network provider[9]. In the context of behavioural advertising, the cookie will enable the ad network provider to recognise a former visitor who returns to that web site or visits any other website that is a partner of the advertising network. Such repeated visits will enable the ad network provider to build a profile of the visitor which will be used to deliver personalised advertising. Because these tracking cookies are placed by a third party that is distinct from the web server that displays the main content of the webpage (i.e. the publisher) they are often referred to as "third party cookies".

Cookies are tied to a domain: a cookie can only be read or modified by a website that comes from a similar domain[10] (e.g. a cookie placed by ad provider a.mysite.com can be read by b.mysite.com but not by ad provider c.another.com). Cookies have different life spans. This lifespan might or might not be extended further in the future upon further visits to the same site (this is a design decision by the programmer). "Persistent cookies" either have a precise expiry date far in the future or until they are manually deleted.

Most internet browsers offer the possibility to block third party cookies. Some browsers support "private" browsing sessions that will automatically destroy all created cookies when the browser window is closed[11].

Some ad networks are replacing or supplementing traditional tracking cookies with new enhanced tracking technologies such as "Flash Cookies" (local shared objects)[12]. Flash cookies cannot be deleted through the traditional privacy settings of a web browser. It has been reported that "Flash Cookies" have been used explicitly as a tool to restore "traditional cookies" that were refused or erased by the data subject[13].

---

7 Other tracking technologies are for example based on the use of IP addresses and browser signatures. The Electronic Frontier Foundation investigated identifiability of the individual browser signature (user agent), including the software used, version, language and installed plug-ins, URL: http://panopticlick.eff.org/). With regard to IP addresses a USA start-up recently announced it had a database of 65 Million IP Addresses connected with name and address data, URL: http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=123280.

8 If a data subject uses different browsers, the cookies will be different for each browser.

9 This alphanumeric text can be used for a large variety of purposes such as memorising preferences, storing session information, or identifying a data subject though a unique identifier.

10 However, there are simple solutions for cooperating parties who wish to get around this restrictions and share cookies with each other. A domain owner can configure his DNS to allow a third party to use one of his sub-domains. The third party will than be able to share certain cookies with the domain owner. Other techniques involve javascript performing additional web requests to yet other servers, allowing even more parties to link or sync their tracking data (http://blog.kruxdigital.com/2010/02/24/cookie-synching/).

11 The latest versions of many popular browsers (*e.g.*, Internet Explorer 8, Google Chrome, Firefox, Safari etc.) support browsing sessions that automatically delete all cookies installed during that session.

12 The W3C is also developing a "DOM Storage" standard that will allow the creation of large local storage of data by scripts on the users' computer.

13 Flash cookies are capable of storing information about the settings and circumvent the user's preferences. See Soltani, Ashkan, Canty, Shannon, Mayo, Quentin, Thomas, Lauren and Hoofnagle, Chris Jay, "Flash Cookies and Privacy" (August 10, 2009). Available at SSRN: http://ssrn.com/abstract=1446862

This practice is known as *respawning*. In this opinion, the term "cookies" will be used to refer to all technologies which are based on the principle of storing and accessing information on the user terminal equipment, unless otherwise noted.

As pointed out above, a single ad network can usually monitor only part of the data subject's internet browsing behaviour because its tracking capability is limited to the set of publishers that link to it. However, another approach was tested in the recent past whereby the ad network entered into a partnership with an ISP in order to monitor the user's browsing content and to insert tracking cookies in all unencrypted web traffic[14]. The Article 29 Working Party is not aware of any current application of this technology in the EU, but it considers that the application of this technology raises serious legal issues beyond the processing of personal data, regardless of the purpose for which the data are being used. The analysis of this advertising technology falls outside the scope of this Opinion.

2.3. Building profiles, types of identifiers

There are two main approaches to building user profiles: *i)* **Predictive profiles** are established by inference from observing individual and collective user behaviour over time, particularly by monitoring visited pages and ads viewed or clicked on. *ii)* **Explicit profiles** are created from personal data that data subjects themselves provide to a web service, such as by registering. Both approaches can be combined. Additionally, predictive profiles may be made explicit at a later time, when a data subject creates login credentials for a website[15].

Ad networks construct predictive profiles by using a combination of tracking techniques, cookie based technologies and data mining software. Gender and age range can be deduced by analysing the pages the data subject visits and the ads to which he or she gravitates. The profile based on analysis of the cookies stored on the terminal equipment of the data subject can be enriched with aggregated data derived from the behaviour of data subjects who exhibit similar behavioural patterns in other contexts. Online advertising systems often classify data subjects into segments, either by their areas of interest or by their marketing categories (examples are "gardening", "body care", "electronics", etc.).

The location of the data subject is also a primary source of target profiling. It can be deduced, for example, from the IP address of the terminals and WiFi access points[16].

3. Legal Framework

3.1. Introduction

Article 5 (1) of Directive 2002/58[17] protects the confidentiality of communications in general. The protection of the confidentiality of communications in the concrete case of the use of cookies and similar devices is primarily laid down in Article 5(3). This Opinion relates and refers to the amended Directive 2002/58 (hereafter, the "ePrivacy Directive" or "amended ePrivacy Directive"). The amended ePrivacy Directive does not have to be implemented by

---

[14] For example, the company Phorm though its technology called Webwise offered a behavioral targeting service that uses deep packet inspection to examine the pages viewed by Internet users. To provide the service, Phorm entered into partnership agreements with ISPs.

[15] Some ad networks allow registered users to view and edit their associated predictive profiles, at least to a certain degree.

[16] Additional location information may be collected from other sources and be used for profiling purposes.

[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 and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

Member States into national law until May 2011. However, the Article 29 Working Party already refers to the amended ePrivacy Directive, because it wishes this Opinion to remain valid after the Directive's implementation and more particularly because it wants to alert stakeholders about the need to fully comply with the amended Article 5(3). Also relevant in this context are Recital 66, adopted when the ePrivacy Directive was amended in 2009 and Recital 24 and 25 of the ePrivacy Directive.

Taking into account the relevance of Article 5(3), it is useful to reproduce the amended text here, with change marks against the previous text:

> *Member States shall ensure that the ~~use of electronic communications networks to~~ stor~~i~~**ing of** information, ~~or to gain~~ 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** ~~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 **for the** provide**r of** ~~to provide~~ an information society service explicitly requested by the subscriber or user **to provide the service**."*

In addition to the ePrivacy Directive, Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter "Directive 95/46/EC") applies to matters not specifically covered by the ePrivacy Directive whenever personal data are processed[18].

3.2. The scope of application of Article 5(3) and Directive 95/46/EC

For those engaged in behavioural advertising, it is useful to know what triggers the obligation to comply with Article 5(3) of the ePrivacy Directive and Directive 95/46/EC respectively. This requires addressing the scope of application of both Directives. In particular, we will first refer to the substantive scope of application of both Directives (3.2.1 and 3.2.2) and to their interaction (3.2.3). Then, we will refer to the territorial scope of application of both Directives (3.2.4).

3.2.1. Substantive scope of application of Article 5(3)

Article 5(3) requires obtaining informed consent to lawfully store information or to gain access to information stored in the terminal equipment of a subscriber or user[19]. Taking into account that (i) tracking cookies are 'information' stored in the data subject's terminal equipment and, (ii) they are accessed by advertising network providers when data subjects visit a partner website, Article 5(3) is fully applicable. Hence, any storage of cookies or similar devices (irrespective of type)[20] and any subsequent use of previously stored cookies to gain access to data subjects' information will have to comply with Article 5(3).

---

[18] See Article 2 of the ePrivacy Directive which says: "*The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1*".

[19] The ePrivacy Directive refers to subscribers and users. Subscribers include both individuals or data subjects (as referred to as in Directive 95/46/EC) as well as legal persons. The word 'user' refers to data subjects that are using an electronic communication service, without necessarily having subscribed to it. For consistency reasons, this Opinion uses, whenever possible, the word 'data subject'.

[20] Article 5(3) is technologically neutral, therefore, it is applicable not only to cookies but also to any other technology used to store or gain access to information stored in their individuals' technical equipment (spyware, malware, etc).

Article 5(3) applies to "information" (stored and/or accessed). It does not qualify such information. It is not a prerequisite for the application of this provision that this information is personal data within the meaning of Directive 95/46/EC. Recital 24 captures the *rationale* of this approach by stating that *"terminal equipment of users…and any information stored on such equipment are part of the private sphere of these users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms*". The protection of an area deemed to be the private sphere of the data subject is what triggers the obligations contained in Article 5(3), not the fact that the information is, or is not, personal data.

The Working Party has already pointed out in WP 29 Opinion 1/2008[21] that Article 5(3) is a general provision, which is applicable not only to electronic communication services but also to any other services when the respective techniques are used. Furthermore, Article 5(3) applies irrespectively of whether the entity that places the cookie is a data controller or a data processor.

3.2.2. Substantive scope of application of Directive 95/46/EC: Processing of personal data

If as a result of placing and retrieving information through the cookie or similar device, the information collected can be considered personal data then, in addition to Article 5(3), Directive 95/46/EC will also apply.

The Article 29 Working Party notes that the behavioural advertising methods described in this Opinion often entail the processing of personal data as defined by Article 2 of Directive 95/46/EC and interpreted by Article 29 Working Party[22]. This is due to various reasons: *i)* behavioural advertising normally involves the collection of IP addresses and the processing of unique identifiers (through the cookie). The use of such devices with a unique identifier allows the tracking of users of a specific computer even when dynamic IP addresses are used. In other words, such devices enable data subjects to be 'singled out', even if their real names are not known. *ii)* Furthermore, the information collected in the context of behavioural advertising *relates to*, (*i.e*. is about) a person's characteristics or behaviour and it is used to influence that particular person[23]. This view is further confirmed if one takes into account the possibility for profiles to be linked at any moment with directly identifiable information provided by the data subject, such as registration related information. Other scenarios that can lead to identifiability are mergers, data losses and the increasing availability on the Internet of personal data in combination with IP addresses.

3.2.3. Interplay between the two Directives

If both Directives apply, a relevant question is to determine the applicable provisions of each Directive. In this regard, Recital 10 of the ePrivacy Directive states that Directive 95/46/EC applies, "*to all matters concerning protection of fundamental rights and freedoms which are not specifically covered by the provisions of this Directive, including the obligations on the controller and the rights of individuals*".

---

21 Opinion 1/2008 on data protection issues related to search engines, adopted on 04.04.2008.

22 See interpretation of the concept of personal data in the Article 29 Working Party Opinion 4/2007 on the concept of personal data, adopted on 20.06.2007.

23 In its Opinion 1/2008 on data protection issues related to search engines, adopted on 4 April, 2008, the Article 29 Working Party confirmed that, in most cases, cookies and IP addresses are to be considered personal data. This Opinion stated "*When a cookie contains a unique user ID, this ID is clearly personal data. The use of persistent cookies or similar devices with a unique user ID allows tracking of users of a certain computer even when dynamic IP addresses are used. The behavioural data that is generated through the use of these devices allows focusing even more on the personal characteristics of the individual concerned*".

This is an application of the doctrine that states that a law governing a specific subject matter (*lex specialis*) overrides a law which only governs a general matter (*lex generalis*)

In line with the above, Article 5(3) of the ePrivacy Directive which deals with informed consent will be directly applicable. Directive 95/46 will be fully applicable except for the provisions that are specifically addressed in the ePrivacy Directive, which mainly correspond to Article 7 of Directive 95/46/EC on the legal grounds for data processing[24]. The remaining provisions of Directive 95/46/EC including the principles regarding data quality, the data subject's rights (such as access, erasure, right to object), confidentiality and security of the processing and international data transfers will be fully applicable.

3.2.4. Territorial scope of application of Article 5(3) and of Directive 95/46/EC

The territorial scope of application of the above framework is determined by a combination of both Article 3(1) of the ePrivacy Directive[25] and Article 4.1 (a) and (c) of Directive 95/46/EC[26].

In earlier opinions the Article 29 Working Party has given guidance regarding the concept of establishment and the use of equipment referred to in Article 4.1 (a) and (c) respectively as determinants for the applicability of Directive 95/46/EC[27]. Such guidance is fully applicable to providers of ad networking services.

3.3. Roles and responsibilities of the different players

As described above, behavioural advertising involves various players, including ad network providers, publishers and advertisers. It is important to assess the role they play in order to establish their obligations under current data protection legislation. In this regard, the Article 29 Working Party notes the following:

Regarding ad network providers:

First, the obligations set up by Article 5(3) of the ePrivacy Directive apply to those who place cookies and/or retrieve information from cookies already stored in the data subjects' terminal equipment. Under Article 5(3), it is irrelevant whether the entity placing or reading the cookie is a data controller or a data processor. In the context of behavioural advertising, such interpretation puts the obligation to obtain informed consent upon ad network providers.

Second, at the same time, when behavioural advertising entails the processing of personal data, ad network providers also play the role of data controller. This is very important insofar as additional obligations stemming from the application of Directive 95/46/EC will be applicable. Ad network providers have complete control over the purposes and means of the processing.

---

[24] The principle of fair and lawful processing of Article 6(1) (a) can also be understood to be included in Article 5(3) insofar as fairness refers to and requires transparency.

[25] The scope of application of ePrivacy Directive is set forth under its Art 3(1) pursuant to which Article 5(3) would apply to the storage or gaining access to information residing in the terminal equipment of data subjects who use public communication networks in the EU.

[26] The two criteria that trigger the application of the Directive (or rather the national law that implements it) are (i) when the data processing is carried out in the context of the activities' of the establishment of a data controller" *ex* Article 4(1)(a) and, (ii) if the controller is not established on EU territory but for purposes of processing personal data makes use of equipment, automated or otherwise, situated on EU territory *ex* Article 4(1)(c).

[27] See WP 56 of 30 May 2002 on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites and more recently Opinion 1/2008 on data protection issues related to search engines, adopted on 4 April, 2008.

They 'rent' space from publishers' web sites to place adverts; they set and/read cookie related information and, in most cases, collect the IP address and possible other data that the browser may reveal. Further, the ad network providers use the information gathered on Internet users' surfing behaviour to build profiles and to select and deliver the ads to be displayed on the basis of this profile. In this scenario, they clearly act as data controllers.

Regarding publishers:

Publishers, among others, rent out space on their websites for ad networks to place adverts. They set up their web sites in a way that visitors' browsers are automatically redirected to the webpage of the ad network provider (which will then send a cookie and serve tailored advertising). This raises the question about their responsibility vis-à-vis the data processing.

As recently pointed out by the Article 29 Working Party[28], whether a publisher can be deemed to be a joint controller with the ad network provider will depend on the conditions of collaboration between the publisher and the ad network provider. In this context, the Article 29 Working Party notes that in a typical scenario where ad network providers serve tailored advertising, publishers contribute to it by setting up their web sites in such a way that when a user visits a publisher's web site, his/her browser is automatically redirected to the webpage of the ad network provider. In doing so, the user's browser will transmit his/her IP address to the ad network provider which will proceed to send the cookie and tailored advertising. In this scenario, it is important to note that publishers do not transfer the IP address of the visitor to the ad network provider. Instead, it is the visitor's browser that automatically transfers such information to the ad network provider. However, this only happens because the publisher has set up its web site in such a way that the visitor to its own web site is automatically re-directed to the ad network provider web site. In other words, the publisher *triggers* the transfer of the IP address, which is the first necessary step that will allow the subsequent processing, carried out by the ad network provider for the purposes of serving tailored advertising. Thus, even if, technically the data transfer of the IP address is carried out by the browser of the individual who visits the publisher web site, it is not the individual who triggers the transfer. The individual only intended to visit the publisher's web site. He did not intend to visit the ad network provider's web site. Currently this is a common scenario.

Taking this into account, the Article 29 Working Party considers that publishers have a certain responsibility for the data processing, which derives from the national implementation of Directive 95/46 and/or other national legislation[29]. This responsibility does not cover all the processing activities necessary to serve behavioural advertising, for example, the processing carried out by the ad network provider consisting of building profiles which are then used to serve tailored advertising. However, the publishers' responsibility covers the first stage, i.e. the initial part of the data processing, namely the transfer of the IP address that takes place when individuals visit their web sites. This is because the publishers facilitate such transfer and co-determine the purposes for which it is carried out, i.e. to serve visitors with tailored adverting. In sum, for these reasons, publishers will have some responsibility as data controllers for these actions. This responsibility cannot, however, require compliance with the bulk of the obligations contained in the Directives.

---

[28] Opinion 1/2010 on the concepts of "controller" and "processor", adopted on 16.02.2010.

[29] The Article 29 Working Party notes that the obligation to inform and other possible obligations may also derive from general principles of law (law of contracts and torts) as well as consumer protection laws related to business-to-consumer commercial practices such as Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'

In this regard, it is necessary to interpret the legal framework in a flexible way by applying only those provisions that are pertinent. Publishers do not hold personal information; so obviously, it would not make sense to apply some of the obligations of the Directive such as the right of access. However, as further described below, the obligation to inform individuals of the data processing is fully applicable to publishers.

In addition to the above, as mentioned in the Article 29 Opinion referred to above, publishers will be joint controllers if they collect and transmit personal data regarding their visitors such as name, address, age, location, etc to the ad network provider. To the extent that publishers act as data controllers they are bound by the obligations arising from Directive 95/46/EC regarding the part of the data processing under their control. In this regard, together with ad network providers, publishers "*shall ensure that the complexity and the technicalities of the behavioural advertising system do not prevent them from finding appropriate ways to comply with controllers' obligations and to ensure data subjects' rights*"[30].

In sum, publishers should be aware that by entering into contracts with ad networks with the consequence that personal data of their visitors are available to ad network providers, they take some responsibility towards their visitors. The breadth of their responsibility, including the extent to which they become data controllers should be analysed on a case by case basis depending on the particular conditions of collaboration with ad network providers, as reflected in the service agreements. Accordingly, the service agreements between publishers and ad network providers should set up the roles and responsibilities of both parties in the light of their collaboration, as described in the agreement.

Regarding advertisers:

When a data subject clicks through on an ad and visits the advertisers' website, the advertiser can track which campaign resulted in the click-through. If the advertiser captures the targeting information (e.g. certain demographic data such as "young mothers" or an interest group such as "extreme sports fan") and combines it with the data subject's onsite surfing behaviour or registration data, then the advertiser is an independent data controller for this part of the data processing.

This Opinion focuses on the data processing operations carried out by the ad network provider and the publisher consisting in serving targeted advertisements. It does not comment on the potential additional data processing operations that may be carried out by advertisers described above.

4. Obligation to obtain prior informed consent

The general rule contained in the first paragraph of Article 5(3) requires Member States to: "*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 article was changed when the ePrivacy Directive was amended in 2009. The changes in the amended version clarify and reinforce the need for users' informed prior consent[31]. The Article 29 Working Party considers that the legal analysis made below is relevant and valid both vis-à-vis the current version of Article 5(3) and the amended Article 5(3).

---

[30] Opinion 1/2010 on the concepts of "controller" and "processor" http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf

[31] This is done in two ways: First, by changing the words "right to refuse" by the need to obtain "consent", as referred to in Directive 95/46/EC and by using the verb in past tense "has been provided".

The following section analyses various ways of meeting the requirements of Article 5(3). After the discussion on consent, there is further guidance on the obligation to provide information.

4.1. The obligation to obtain data subjects' prior consent to engage in behavioural advertising

Pursuant to Article 5.(3), an ad network provider who wishes to store or gain access to information stored in a user's terminal equipment is allowed to do so if: *i*) it has provided the user with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing and; *ii)* it has obtained the user's consent to the storage of or access to information on his or her terminal equipment, after having provided the information requested under *i)*.

It follows from the literal wording of Article 5.(3) that: *i)* consent must be obtained *before* the cookie is placed and/or information stored in the user's terminal equipment is collected, which is usually referred to as prior consent and *ii)* informed consent can only be obtained if prior information about the sending and purposes of the cookie *has been given to the user*. In this context, it is important to take into account that for consent to be valid whatever the circumstances in which it is given, it must be freely given, specific and constitute an informed indication of the data subject's wishes. Consent must be obtained before the personal data are collected, as a necessary measure to ensure that data subjects can fully appreciate that they are consenting and what they are consenting to. Furthermore, consent must be revocable.

The next sub-sections analyse whether consent by the way of browser settings and opt-out options provided by ad network providers meet the requirements of Article 5(3).

4.1.1. Consent by the way of browser settings

Publishers and ad network providers engaged in behavioural advertising place tracking cookies in a data subject's terminal equipment when the data subject accesses a website that is part of the ad network. This happens unless the user's browser is set to reject cookies. In practice, once the cookie is placed and the data subject is browsing the web page where the ad has been served, he or she is put in a position to learn about the cookies and how to set the browser in order to control cookies. This is done by publishers and ad network providers. These controllers usually provide information in their general terms and conditions and/or privacy policies about third party cookies used for behavioural advertising. The information may include the basic uses/purposes of such cookies and how they can be avoided by setting the browser. However, this practice does not meet the requirements of Article 5(3), particularly in its amended version, which places emphasis on providing prior information and obtaining prior consent (prior to the starting of the processing).

Recital 66 of the amended ePrivacy Directive indicates that the user's consent may be expressed by using the appropriate settings of a browser or other application, "*where it is technically possible and effective, in accordance with the relevant provisions of Directive 95/46/EC*". This is not an exception to Article 5(3) but rather a reminder that, in this technological environment, consent can be given in different ways - where technically possible, effective and in accordance with the other relevant requirements for valid consent. In this context, a relevant question is to determine the conditions under which the browser settings will meet the requirements of Directive 95/46/EC, and thus constitute a valid consent "*in accordance with Directive 95/46"*. The Article 29 Working Party considers that this will happen in very limited circumstances because:

First, based on the definition and requirements for valid consent *ex* Article 2 (h) of Directive 95/46/EC, generally speaking data subjects cannot be deemed to have consented simply because they acquired/used a browser or other application which by default enables the collection and processing of their information. Average data subjects are not aware of the tracking of their online behaviour, the purposes of the tracking, etc. They are not always aware of how to use browser settings to reject cookies, even if this is included in privacy policies. It is a fallacy to deem that on a general basis data subject inaction (he/she has not set the browser to refuse cookies) provides a clear and unambiguous indication of his/her wishes. As pointed out by the Article 29 Working Party Opinion 1/2008 referred to earlier "*The responsibility for [cookie] processing cannot be reduced to the responsibility of the user for taking or not taking certain precautions in his browser settings.*" Currently, of the four major browsers, only one browser blocks 3d party cookies by default from the moment the browser is installed. The other three major browsers have as a default setting to allow all cookies. In these cases, cookies are being sent and information is collected prior to obtaining consent, thus clashing with the need for prior consent[32].

Second, for browsers settings to be able to deliver informed consent, it should not be possible to "bypass" the choice made by the user in setting the browser. However, in practice deleted cookies may be easily "respawned" by so-called flash cookies, enabling the ad network provider to continue monitoring the user. The availability and increasing use of such technology challenges the ability of browser settings to deliver informed, valid and effective consent.

Finally, consent by browser setting to receive cookies in bulk implies that users will accept future processing, possibly without any knowledge of the purposes or uses of the cookie. Consent in bulk for any future processing without knowing the circumstances surrounding the processing cannot be valid consent[33].

Therefore, in order for browsers or any other application to be able to 'deliver' valid consent, they must overcome the above problems. Effectively, this means that:

(a) Browsers or other applications which by default reject 3rd party cookies and which require the data subject to engage in an affirmative action to accept both the setting of and continued transmission of information contained in cookies by specific web sites may be able to deliver valid and effective consent. By contrast, if the browser settings were predetermined to accept all cookies, such consent would not comply with Article 5(3) insofar as, in general, such consent cannot constitute a true indication of the data subject wishes. Such consent would neither be specific nor prior (to the processing). Whereas a given data subject could indeed have decided to keep the settings to accept all 3rd party cookies, it would not be realistic for ad network providers to assume that the vast majority of data subjects who have their browsers "set" to accept cookies, effectively exercised this choice.

---

[32] A further complication is that the three browses referred above still transmit existing cookie information even when the browser settings are set to reject (new) 3d party cookies. In other words, information about cookies which have been placed before setting the browser to reject cookies will continue being sent to the ad network provider. Only one major browser currently allows users to both block the setting and the transmission of 3d party cookie data (i.e., including cookies placed before the setting of the browser to reject cookies). This has as consequence that also cookies that have been set as first-party (when visiting the single website of, for example,. a search engine or a social networking site) can still be read by that site when the user visits a site that has partnered with that first website.

[33] As the Article 29 Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, adopted on 25.11.2005 said in the context of future data transfers "The importance of consent constituting a positive act excludes de facto any system whereby the data subject would have the right to oppose the transfer only after it has taken place: specific consent to a transfer must genuinely be required for the transfer to take place".

(b) Browsers, together or in combination with other information tools, including the cooperation of ad network providers and publishers, should convey clear, comprehensive and fully visible information in order to ensure that consent is fully informed. To meet the requirements of Directive 95/46/EC browsers should convey, on behalf of the ad network provider, the relevant information about the purposes of the cookies and the further processing. So, generic warnings without explicit references to the ad network which is placing the cookie are unsatisfactory.

The Article 29 Working Party is of the view that unless the above requirements are met, providing information and, to some extent, facilitating the user's ability to reject cookies (by explaining how this can be done) cannot generally be deemed as informed consent *ex* Article 5(3) of the ePrivacy Directive and also in light of Article 2(h) of Directive 95/46/EC.

Given the importance that browser settings play in ensuring that data subjects effectively give their consent to the storage of cookies and the processing of their information, it seems of paramount importance for browsers to be provided with default privacy-protective settings. In other words, to be provided with the setting of 'non-acceptance and non-transmission of third party cookies'. To complement this and to make it more effective, the browsers should require users to go through a privacy wizard when they first install or update the browser and provide for an easy way of exercising choice during use. The Working Party 29 calls upon browser makers to take urgent action and coordinate with ad network providers.

4.1.2. Consent and the exercise of opt-out options

Ad network providers increasingly offer "opt-out" mechanisms enabling users to opt-out from receiving targeted advertising[34]. By relying on this mechanism, the data subject must go to the website of the ad network provider/s and indicate to the ad network provider/s that they wish to opt-out from being tracked for the purposes of being served targeted advertisements. These mechanisms aim at complementing and, to some extent, fixing the problems described above regarding consent by browser settings.

Such cookie-based opt-out mechanisms are welcome and to be encouraged insofar as they facilitate current data subjects' technical possibilities to opt-out. However, such opt-out mechanisms do not in principle deliver data subjects' consent. Only in very specific, individual cases, could implied consent be argued. This could be the case when an experimented user, who is aware of the practice of behavioural advertising, knows that he/she can opt out from it, but chooses to exercise a volitional act of not opting-out (particularly if this is done before any cookie has been sent to the user). However, this mechanism is not an adequate mechanism to obtain average users informed consent. The reasons are similar to those indicated above in the context of browser setting, namely:

First, in general users lack the basic understanding of the collection of any data, its uses, how the technology works and more importantly how and where to opt-out. As a result, in practice very few people exercise the opt-out option, not because they have made an informed decision to accept behavioural advertising, but rather because they do not realise that by not using the opt out, they are in fact accepting.

Second, consent means active participation of the data subject prior to the collection and processing of data. The opt-out mechanism often refers to a 'non' reaction of the data subject after such processing has already started. Furthermore, under opt-out mechanism there is no

[34] See for example the opt-out option provided by Network Advertising Initiative which offers the possibility to opt out from various networks: http://www.networkadvertising.org/managing/opt_out.asp

active participation; simply the will of the data subject is assumed or implied. This does not meet the requirements for legally effective consent.

In light of the above, the Article 29 Working Party considers that cookie-based opt-out mechanisms do not provide average users with the effective means to consent to receive behavioural advertisement. In this regard, they fail to fulfil the requirement of Article 5(3).

4.1.3. Prior opt in consent mechanisms are better suited to deliver informed consent

The Article 29 Working Party is of the view that prior opt-in mechanisms, which require an affirmative data subject's action to indicate consent before the cookie is sent to the data subject, are more in line with Article 5(3). In a reference to consent as legal grounds for processing, the Article 29 Working Party recently confirmed these views "*The technological developments also ask for a careful consideration of consent. In practice, Article 7 of Directive 95/46/EC is not always properly applied, particularly in the context of the internet, where implicit consent does not always lead to unambiguous consent (as required by Article 7 (a) of the Directive). Giving the data subjects a stronger voice 'ex ante', prior to the processing of their personal data by others, however requires explicit consent (and therefore an opt-in) for all processing that is based on consent.*"[35]

In a previous Opinion which discussed this issue, the Working Party 29[36] recommended the use of specific messages: *"In the case of cookies, the user should be informed when a cookie is intended to be received, stored or sent...The message should specify, in generally understandable language, which information is intended to be stored in the cookie, for what purpose as well as the period of validity of the cookie."* After having received such information, the data subject should be offered the possibility to indicate whether he/she wants to be profiled for the purposes of behavioural advertising.

The Article 29 Working Party is conscious of the current practical problems related to obtaining consent, particularly if consent is necessary every time a cookie is read for the purposes of delivering targeted advertising. To avoid this problem, in accordance with Recital 25 of the ePrivacy Directive ("*the right to refuse (cookies) may be offered once for the use of various devices to be installed on the user's terminal equipment….during subsequent connections*"), users' acceptance of a cookie could be understood to be valid not only for the sending of the cookie but also for subsequent collection of data arising from such a cookie. In other words, the consent obtained to place the cookie and use the information to send targeting advertising would cover subsequent 'readings' of the cookie that take place every time the user visits a website partner of the ad network provider which initially placed the cookie.

However, taking into account that *i)* this practice would mean that individuals accept to be monitored "once for ever," and, *ii)* individuals might simply 'forget' that, for example, a year ago, they agreed to be monitored; the Working Party considers that some safeguards should be implemented. In particular, the Article 29 Working Party proposes three courses of action:

First, to limit the scope of the consent in terms of time. Consent to be monitored should not be 'for ever' but it should be valid for a limited period of time, for example, to one year. After this period, ad network providers would need to obtain a new consent. This could be achieved if cookies had a limited lifespan after they have been placed in the user's terminal equipment (and the expiry date should not be prolonged).

---

[35] The Article 29 Working Party acknowledges the work made by some associations such as The Future of Privacy in the context of promoting the use of icons for information purposes.

[36] Recommendation 1/99 on invisible and automatic processing of personal data on the internet: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1999/wp17en.pdf.

Second, the risks outlined above would be further mitigated with additional information practices, further addressed below under Section 4.2.1.

Third, freely given consent can always be revoked. Data subjects should be offered the possibility to easily revoke their consent to being monitored for the purposes of serving behavioural advertising. In this regard, the need to provide clear information about this possibility and how to exercise it is essential (see below under Section 4.2)

The Article 29 Working Party encourages the advertising industry to implement the above or alternative methods entailing a prior affirmative action from the users towards accepting *i*) the storage of the cookie and *ii*) the use of the cookie to track him/her across websites in order to deliver behavioural advertising. This may include the design of browsers and browser technology as well.

4.1.4 Informed consent: children

In Opinion 2/2009 the Article 29 Working Party has addressed the protection of personal data of children[37].The problems related to obtaining informed consent are further emphasized as far as children are concerned. In addition to the requirements described above (and below) for consent to be valid, in some cases children's consent must be provided by their parents or other legal representatives. In the case in point this means that ad network providers would need to provide notice to parents about the collection and the use of children's information and obtain their consent before collecting and further using their information for the purposes of engaging in behavioural targeting of children[38].

In the light of the above and also taking into account the vulnerability of children, the Article 29 Working Party is of the view that ad network providers should not offer interest categories intended to serve behavioural advertising or influence children.

4.2. The obligation to provide information in the context of behavioural advertising

Transparency is a key condition for individuals to be able to consent to the collection and further processing of their data. As outlined above, 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. 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.

4.2.1 Which information must be provided and by whom?

Article 5(3) states that the user must be provided with information, *"in accordance with Directive 95/46/EC, inter alia about the purposes of the processing"*. Article 10 of Directive *95/46/EC* deals with the provision of this information[39].

With regard to behavioural advertising, data subjects should informed, *inter alia*, about the identity of the advertising network provider and the purposes of the processing. The data

---

37 Opinion on the protection of children's personal data (General Guidelines and the special case of schools): http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp160_en.pdf

38 This is in addition to applicable advertising legislation and standards.

39 It requires notably the provision of the identity of the controller, the purposes of the processing; as well as the recipients of the data and the existence of the right of access in so far as such further information is necessary, to guarantee fair processing..

subject should be clearly informed that the cookie will allow the advertising provider to collect information about visits to other websites, the advertisements they have been shown, which ones they have clicked on, timing etc.

There should be a simple explanation on the uses of the cookie to create profiles in order to serve targeted advertising. Recital 25 of the ePrivacy Directive requires notices to be provided in a *"clear and comprehensive"* manner. Statements such as "*advertisers and other third parties may also use their own cookies or action tags*" are clearly not sufficient.

Regarding how this information should be provided, Recital 25 requires it to be "*as user friendly as possible"*. The Article 29 Working Party considers that providing a minimum of information directly on the screen, interactively, easily visible and understandable, would be the most effective way to comply with this principle[40]. It is important for information to be easily accessible and highly visible. This essential information may not be hidden in general terms and conditions and/or privacy statements.

The Article 29 Working Party acknowledges that technically there may be different ways to provide information and welcomes creativity in this area. The Article 29 Working Party is aware that some ad network providers have started developing new ways to provide information and welcomes these developments. Icons placed around advertising on the publisher's website with links to additional information, are examples of such developments which the Working Party finds both positive and necessary.

Taking into account the possibility outlined above under Section 4.1.3 for individuals to accept the monitoring once, to cover subsequent future readings of the cookie, the Article 29 Working Party considers it essential for ad network providers to find ways to inform individuals *periodically* that the monitoring is taking place. Unless data subjects are given clear and unambiguous reminders, by easy means, of the monitoring, it is quite likely that after a certain period of time, they may not longer be aware that it is still taking place and that they consented to it. In this regard, the Article 29 Working Party would be very supportive of the creation of a symbol and related messages that would alert consumers that an ad network provider monitors their user browsing behaviour for the purposes of serving targeted advertising. This symbol would be very helpful not only to remind individuals of the monitoring but also to control whether they want to continue or revoke their consent.

Another relevant question is *who should provide the information* - should it be provided by the publisher or by the ad network provider or both? The outcome should be that data subjects receive easily accessible and highly visible information. As further developed below, for this, the cooperation of both ad network providers and publishers seem essential.

The Article 29 Working Party notes that pursuant to the working of Article 5(3) of the ePrivacy Directive, the obligation to provide the necessary information and obtain data subjects' consent ultimately lies with the entity that sends and reads the cookie. In most cases, this is the ad network provider. When publishers are joint-controllers, for example in those cases where they transfer directly identifiable information to ad network providers, they are also bound by the obligation to provide information to data subjects about the data processing.

In addition, as noted above under Section 3.3, publishers share with ad network providers certain responsibility for the data processing that happens in the context of serving behavioural advertising. More particularly, this responsibility covers the first stage of the

---

[40] This is in line with WP 29 previous guidance, see WP 43 Recommendation 2/2001 on certain minimum requirements for collecting personal data on-line in the European Union adopted on 17 May 2001, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp43en.pdf

processing, i.e. the transfer of the IP address to ad network providers that takes place when individuals visit their web sites and are re-directed to the ad network provider web site.

As a result of such responsibility, publishers have certain obligations vis-à-vis data subjects that stem mainly from the Directive 95/46/EC[41]. Particularly, the Article 29 Working Party considers that publishers are bound by the obligation to provide information to data subjects about the data processing that takes place as a result of the re-directing of their browser and also about the purposes for which the information will be used later on by ad network providers. The information should refer not only to the transfer of IP address for the purposes of displaying acts but also to further data processing carried out by the ad network providers, including the setting up of cookies.

Obviously, the Article 29 Working Party is not suggesting that information must be provided twice (once by the ad network provider and the other by the publisher). The Article 29 Working Party considers that this is an area where there is a clear need for cooperation between ad network providers and publishers so that they decide who will provide the information and how this will be done. It therefore calls upon ad network providers and publishers to spare no effort in order to provide the most effective notices and ensure the maximum level of awareness among internet users as to how behavioural advertising works in each particular situation. The need for this interaction is further emphasized if one takes into account that ad network providers are, in principle, invisible to data subjects. Instead, the user interaction is with the visited web site, i.e. the publisher's web site. For this reason, from a user's perspective, it is more intuitive if they receive the notice from the publisher's web site. This can be done in different ways. For example, if the publisher provides space on its web site, in which ad providers can display the required information.

Data protection authorities in the exercise of their duties will consider appropriate awareness-raising measures about these practices and the correspondent data subjects' rights.

5 Other Obligations and Principles derived from Directive 95/46/EC

In addition to Article 5(3), data controllers must ensure compliance with all the obligations that arise from Directive 95/46/EC that do not overlap with Article 5 (3) among others, they must ensure:

5.1. Obligations regarding special categories of data

Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership or data concerning health or sex life is considered sensitive *ex* Article 8 of Directive 95/46/EC. The Article 29 Working Party sees serious risks to infringe the personal data of individuals if this type of information is used for the purposes of serving behavioural advertising. Any possible targeting of data subjects based on sensitive information opens the possibility of abuse. Furthermore, given the sensitivity of such information and the possible awkward situations which may arise if individuals receive advertising that reveals, for example, sexual preferences or political activity, offering/using interest categories that would reveal sensitive data should be discouraged.

[41] In addition, the Article 29 Working Party notes that publishers may be liable under general principles of law (law of contracts and torts) as well as consumer protection laws related to business-to-consumer commercial practices to inform individuals insofar as the data processing and monitoring takes place as a result of their action to re-direct them to the ad network provider.

However, if nevertheless, ad network providers offer and use interest categories that reveal sensitive information, they must comply with Article 8 of Directive 95/46/EC. For example, if an ad network provider processes individual behaviour in order to 'place him/her' in an interest category indicating a particular sexual preference they would be processing sensitive data under Article 8 of Directive 95/46/EC. This Article prohibits the processing of sensitive data except in certain, specific circumstances. In this context, the only available legal ground that would legitimize the data processing would be explicit, separate prior opt-in consent *ex* Article 8(2)(a). The requirement for a separate, affirmative prior indication of the data subjects' agreement means that in no case would an opt-out consent mechanism meet the requirement of the law. It also means that such consent could not be obtained thorough browser settings. To lawfully collect and process this type of information, ad network providers would have to set up mechanisms to obtain explicit prior consent, separate from other consent obtained for processing in general.

5.2. Compliance with the principles relating to data quality

Article 6 of 95/46/EC sets forth various principles which must be respected by the data controller. In this context, the following are particularly relevant:

The Article 29 Working Party is aware that profiles collected and used for behavioural advertising could potentially be used for purposes other than advertising. They could potentially be used for the development of new services whose nature is as yet undecided.

However, the above is conditioned to the compliance of Article 6(1)(b) setting forth the ***purpose limitation principle***. This principle prohibits the processing of personal data which is not compatible with the purposes that legitimised the initial collection. In other words, incompatible secondary uses of the information collected and stored for behavioural advertising would contradict Art 6(b) of Directive 95/46/EC. For example, if ad networks form part of a group of companies that provide multiple services, in principle the ad network can not use the data collected for behavioural advertising for such other services (unless it can be demonstrated that the purposes are compatible). For the same reasons, ad networks can not enrich the information gathered for the purposes of behavioural advertisement with other information.

If ad network providers want to use information gathered for behavioural advertisement for secondary, incompatible purposes, for example across services, they need additional legal grounds to do so *ex* Article 7 of Directive 95/46/EC. Hence, they will need to inform data subjects and, in most cases, obtain their consent *ex* Article 7(a).

Article 6(1) (e) requires data to be deleted when it is no longer necessary for the purpose for which the data were collected (***retention principle***). Compliance with this principle requires limiting the storage of information. Accordingly, companies must specify and respect express timeframes under which data will be retained.

Pursuant to the above, information about users' behaviour has to be eliminated if it is no longer needed for the development of a profile. Indefinite or overly long retention periods contradict Article 6(1)(e) of the Directive. The Article 29 Working Party has observed that retention periods of major ad network providers vary, with some companies using an indefinite period and others limiting the retention periods to three months.

Accordingly, the Article 29 Working Party calls upon ad network providers to implement policies to ensure that information collected each time a cookie is read is immediately deleted or anonymised once the necessity for retaining it has expired. Each data controller needs to be able to justify the necessity for a given retention period. The Article 29 Working Party calls

upon ad network providers to provide reasons that justify the conservation period that they consider necessary in the light of the purposes sought by the data processing.

If/when an individual ask for a deletion of his/her profile or if he/she exercises his/her right to withdraw the consent, these actions require the ad network provider to erase or delete promptly the data subject's information insofar as the ad network provider ceases to have the necessary legal grounds (i.e. the consent) allowing the processing.

5.3. Data subjects rights

Data controllers should enable individuals concerned by the processing to exercise their rights of access, rectification, erasure and to object as laid out in Articles 12 and 14 of the Data Protection Directive.

The Article 29 Working Party is aware of the initiatives of ad network providers consisting in offering access to interest categories that data subjects have been labelled with based on the cookie ID number[42]. These new tools enable users not only to access the interest categories that related to them but also modify them and erase them.

The Article 29 Working Party welcomes these initiatives which contribute to making the rights of individuals to easily access and correct their personal data effective. The Article 29 Working Party urges ad network providers to put in place procedures to inform individuals about these tools and to make them as visible as possible to data subjects so that average users are de facto empowered to use them.

5.4. Other obligations

Article 17 of the Directive imposes the obligation upon data controllers and processors to apply ***technical and organisational measures*** to protect personal data against accidental or unlawful destruction loss, disclosure, and other forms of unlawful processing. Compliance with the security obligations will require ad network providers to implement state of the art technical and organisational measures to ensure the security and confidentiality of the information.

Pursuant to Article 18 of Directive 95/46/EC, data controllers may have to ***notify the processing*** of personal data to data protection authorities, unless they are exempt. Accordingly, if applicable under national law, ad network provides must notify the data processing. In addition, if the data is transferred outside the EU, for example, to servers located in third countries, ad network providers must ensure compliance with the provisions on transfers of personal data to third countries (Art 25 and 26 Directive 95/46/EC).

6. Conclusions and Recommendations

Behavioural advertising techniques enable advertisers, mainly ad providers, to track individuals when they surf the internet, to build profiles and to use them to serve tailored advertising. In most cases, individuals are simply unaware that this is happening.

The Article 29 Working Party 29 is deeply concerned about the privacy and data protection implications of this increasingly widespread practice. Whilst data protection legislation requires, among other things, obtaining informed consent from individuals to engage in this

---

[42] See Yahoo's Ad Interest Manager at http://info.yahoo.com/privacy/us/yahoo/opt_out/targeting/ Also, see Google's Interest-Based Advertising at http://www.google.com/ads/preferences/html/about.html.

practice, in reality it is very doubtful whether average individuals are aware of, much less that they consent to, being monitored to receive tailored advertising.

So far, the ways in which the industry has provided information and facilitated individuals to control whether they want to be monitored have failed. Notices provided in general terms and conditions and/or privacy policies, often drafted in rather obscure ways fall short of the requirements of data protection legislation. In some Member States industry has made some efforts to complement existing law with self-regulation. Such efforts are welcome as they specify the general principles contained in the regulatory framework. However, the Article 29 Working Party considers that there is a long way to go. Industry should step up efforts to comply with the reinvigorated applicable laws.

With this Opinion the Article 29 Working Party wishes to guide stakeholders, particularly ad network providers and publishers to comply with the applicable legal framework as interpreted herein. Towards this end, the present Opinion expresses the Article 29 Working Party views on how to interpret the applicable data protection legal framework to the practice of behavioural advertisement. It also calls upon industry to put forward technical and other means to comply with the framework as described herein and to exchange views with the Article 29 Working Party regarding such means. At the end of a certain "discussion" period, the Article 29 Working Party will evaluate the situation and take the necessary and appropriate measures. Meanwhile, the Article 29 Working Party calls upon the relevant parties to implement the recommendations described below.

6.1. Applicable laws

- The EU legal framework for the use of cookies is primarily laid down in Article 5(3) of the ePrivacy Directive[43].

- Article 5(3) applies whenever "information" such as a cookie is stored or retrieved from the terminal equipment of an internet user. It is not a prerequisite that this information is personal data.

- In addition, Directive 95/46/EC applies to matters not specifically covered by the ePrivacy Directive whenever personal data are processed. Behavioural advertising is based on the use of identifiers that enable the creation of very detailed user's profiles which, in most cases, will be deemed personal data.

6.2. Jurisdiction, territorial issue – establishment

- The Directive 95/46/EC applies to the data processing that takes place when publishers and ad network providers engage in behavioural advertising *ex* Article 4.1(a) and (c) of Directive (95/46/EC) and *ex* Art 3 of the ePrivacy Directive. Existing Article 29 Working Party guidance on this issue is fully applicable.

6.3. Roles and responsibilities

- **Ad network providers** are bound by the obligations of Article 5(3) of the ePrivacy Directive insofar as they place cookies and/or retrieve information from cookies already stored in the data subjects' terminal equipment. They are also data controllers insofar as they determine the purposes and the essential means of the processing of data.

[43] The amended ePrivacy Directive must be implemented by May 2011

- ***Publishers*** have certain data controller related responsibilities regarding the processing that takes place in the first phase of the processing, i.e., when by virtue of the way they set up their web sites they trigger the transfer of the IP address to ad network providers (which enable the further processing). Such responsibility entails some, limited data protection obligations (see below). In addition, when/if publishers transfer directly identifiable personal data to ad network providers themselves, they will be deemed joint controllers.

6.4 Obligations and rights

Regarding ad network providers:

- Article 5(3) of the ePrivacy Directive which sets up an obligation to obtain prior informed consent applies to ad network providers.

- Browser settings may only deliver consent in very limited circumstances. Notably, if browsers are set up by default to reject all cookies (having the browser set to such an option) and the user has changed the settings to affirmatively accept cookies, for which he has been fully informed about the name of the data controller, the processing its goals and the data that is collected. Therefore, the browser must either alone or in combination with other means effectively convey clear, comprehensive and fully visible information about the processing.

- Ad network providers should encourage and work with browser manufacturers/developers to implement privacy by design in browsers.

- Cookie-based opt-out mechanisms in general do not constitute an adequate mechanism to obtain informed user consent. In most cases user's consent is implied if they do not opt out. However, in practice, very few people exercise the opt-out option, not because they have made an informed decision to accept behavioural advertising, but rather because they do not realise that the processing is taking place, much less how to exercise the opt out.

- Ad network providers should swiftly move away from opt-out mechanisms and create prior opt-in mechanisms. Mechanisms to deliver informed, valid consent should require an affirmative action by the data subject indicating his/her willingness to receive cookies and the subsequent monitoring of their surfing behaviour for the purposes of sending him tailored advertising.

- In accordance with Recital 25 of the ePrivacy Directive, a users' acceptance to receive a cookie could also entail his/her acceptance for the subsequent readings of the cookie, and hence for the monitoring of his/her internet browsing. It would not be necessary to request consent for each reading of the cookie. However, to ensure that data subjects remain aware of the monitoring over time, ad network providers should*: i)* limit in time the scope of the consent; *ii)* offer the possibility to easily revoke their consent to being monitored for the purposes of serving behavioural advertising and *iii)* create a symbol or other tools which should be visible in all the web sites where the monitoring takes place (the website partners of the ad network provider). This symbol would not only remind individuals of the monitoring but also help them to control whether they want to continue being monitored or wish to revoke their consent.

- Network providers should ensure compliance with the obligations that arise from Directive 95/46/EC which do not directly overlap with Article 5(3), namely, the purpose limitation principle, and security obligations.

- In addition, the ad network providers should enable individuals to exercise their rights of access and rectification and erasure. The Article 29 Working Party welcomes the practice of some ad network providers to offer data subjects the possibility to access and modify the interest categories in which they have been classified.

- Ad network providers should implement retention policies which ensure that information collected each time that a cookie is read is automatically deleted after a justified period of time (necessary for the purposes of the processing). This also applies for alternative tracking technologies used for behavioural advertising such as JavaScript installed in the user's browser environment.

Ad network providers and publishers:

- Providing highly visible information is a precondition for consent to be valid. Mentioning the practice of behavioural advertising in general terms and conditions and/or privacy policies can never suffice. In this regard and taking into account the average low level of knowledge about the practice of behavioural advertising, efforts should be applied to change this situation.

- Ad network providers/ publishers must provide information to users in compliance with Article 10 of Directive 95/46/EC. In practical terms, they should ensure that individuals are told, at a minimum, who (i.e. which entity) is responsible for serving the cookie and collecting the related information. In addition, they should be informed in simple ways that (a) the cookie will be used to create profiles; (b) what type of information will be collected to build such profiles; (c) the fact that the profiles will be used to deliver targeted advertising and (d) the fact that the cookie will enable the user's identification across multiple web sites.

- Network providers/ publishers should provide the information directly on the screen, interactively, if needed, through layered notices. In any event it should be easily accessible and highly visible.

- Icons placed on the publisher's website, around advertising, with links to additional information, are good examples. The Article 29 Working Party urges the network providers/ publisher industry to be creative in this area.

Done at Brussels, on 22 June 2010

For the Working Party
The Chairman
Jacob KOHNSTAMM