02005/11/EN
WP 188

Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising

Adopted on 08 December 2011

Online Behavioural Advertising (**OBA**) ist ein großes Thema.
Internationale Verbände haben im April 2011 Stellung bezogen.
Dies wird hier kommentiert und kritisiert.

Der Ansatz von www.youronlinechoices.eu führe NICHT zu compliance,
weil ein "opt-out" eben keine Einwilligung darstellt.

- cookies OHNE Personenbezug fallen unter die EU-Cookie-Richtlinie (Seite 8)
- cookies zum Login etc. und zum Warenkorb bedürfen keiner Einwilligung
- Browsereinstellungen sind keine Einwilligung (Seite 10)

Zielführend ist ein "opt-in" Cookie, dass als Einwilligung zählen kann.

TABLE OF CONTENTS

I. INTRODUCTION

In November 2009, the European Parliament and Council adopted the Directive 2009/136/EC. This directive revised the 2002 e-Privacy Directive (2002/58/EC). One of the key changes concerns the mechanisms for implanting information in the user's terminal device. The existing opt-out regime, where a user can object to the processing of information collected via terminal equipment (such as 'cookies') was rejected. Instead, the standard became informed consent. These changes play an important role in online behavioural advertising as the industry relies heavily on cookies and similar technologies that store and gain access to information in the user's terminal device.

This requirement for consent reflected a growing concern amongst citizens, politicians, data protection authorities, consumer organisations and policy-makers that the technical possibilities to track individual internet behaviour over time, across different websites, were rapidly increasing. Furthermore, the possibilities offered to citizens to protect their private life and their personal data against this type of tracking were not keeping pace with this growth. By 2009, policy-makers had strong doubts on the possibility to rely on the relevant advertising industry to increase public awareness and user choice with regard to online behavioural advertising. Many public surveys showed, and continue to show, that the average internet user is not aware that his/her behaviour is being tracked with the help of cookies or other unique identifiers, by whom or for what purpose. This lack of awareness contrasts sharply with the increasing dependence of many European citizens on access to internet for ordinary everyday activities such as shopping, reading, communicating with friends and searching for information. The internet is also rapidly replacing several offline activities, such as access to some public services. The rapid replacement of 'fixed' internet access by mobile access has even further complicated the ability of internet users to protect themselves with technical means.

Soon after informed consent became the European legal norm, the Article 29 Working Party (hereinafter Article 29 WP) adopted Opinion 2/2010 on Online Behavioural Advertising (OBA)[1] (hereinafter Opinion 2/2010). The opinion describes the roles and responsibilities of the different actors engaged in online behavioural advertising and clarifies the applicable legal framework. The opinion focuses on the tracking of internet behaviour over time, across different websites as the source of the most important data protection concerns with regard to OBA.

In April 2011 the relevant actors engaged in online behavioural advertising, represented by both the European Advertising Standards Alliance (EASA) and the Internet Advertising Bureau Europe (IAB), adopted a self-regulatory Best Practice Recommendation on online behavioural advertising (hereinafter "EASA/IAB Code")[2]. In August 2011, the Article 29 WP sent an open letter[3] to EASA and IAB outlining the data protection concerns surrounding the opt-out approach suggested within the

1 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf

2 http://www.easa-alliance.org/binarydata.aspx?type=doc/EASA_BPR_OBA_12_APRIL_2011_CLEAN.pdf/download

3 Letter from the Article 29 Working Party addressed to Online Behavioural Advertising (OBA) Industry regarding the self-regulatory Framework, 3 August 2011 http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2011/20110803_letter_to_oba_annexes.pdf

EASA/IAB Code. In a subsequent meeting with the Article 29 WP, representatives of EASA and IAB stated that "the Code was primarily intended to create a level playing field" and that its purpose was not to achieve compliance with the revised e-Privacy Directive[4].

The Article 29 WP welcomes –as already stated in Opinion 2/2010– the self-regulatory initiatives of the Industry in the area of behavioural advertising. The EASA/IAB Code indeed includes some interesting approaches (such as Principle V – Education) which can make the consent mechanisms more effective if they are further developed and implemented. However, the EASA/IAB Code per se is not adequate to ensure compliance with the current applicable European data protection legal framework. In order to prevent any misunderstanding, the Article 29 WP has decided to provide specific analysis on the extent to which this Code, as complemented by the website www.youronlinechoices.eu, complies with the relevant legal provisions.

More specifically, the current opinion focuses on the first two principles of the EASA/IAB Code and its practical implementation in www.youronlinechoices.eu, namely Principle I (Notice) and Principle II (User Choice). In addition, some other principles of the Code, as well as further areas of concern (e.g. data retention) are also discussed. Moreover, the Article 29 WP takes this opportunity to highlight the difference between tracking cookies and other kinds of cookies which may be exempted from consent, providing practical examples of exempted cookies, as well as highlighting possible approaches to legally receive consent where required.

II. ANALYSIS OF THE OBA BEST PRACTICE RECOMMENDATION

II.1 Notice (Principle I)

Under Article 5(3) of the revised e-Privacy Directive, consent must be informed. This in practice means that the user must have given his/her consent to store information or gain access to information stored in his/her terminal equipment after having been provided with clear and comprehensive information in accordance with Directive 95/46/EC, *inter alia*, about the purposes of the processing. Therefore, in order to comply with the legislation, the relevant information notice must be provided directly to the users in a clear and understandable form before the processing takes place. It is not enough for information to be "available" somewhere in the website that the user visits.

Under the EASA/IAB Code, an icon will be used as an information notice for behavioural advertising. In the current implementation of the Code, the icon is linked to an information website, www.youronlinechoices.eu. On this website, users can signal their willingness to opt out by selecting specific company names from a list of different advertising networks.

[4] Press release Article 29 Working Party 14 September 2011 http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20110914_press_release_oba_industry_final_en.pdf

In the present context and taking into account the current lack of knowledge and awareness of the web users with regard to behavioural advertising, the above-mentioned icon approach is not sufficient in itself to properly inform the users about the use of cookies in the sense of Article 5(3). This is due to the following reasons:

a) Although in the future the icon may be widely recognized, currently average users will not be able to recognize the icon's underlying meaning without any additional language. However, the icon could be useful as a means to complement other forms of information notice, by providing links to further information on user rights and serving as a constant reminder to the users that they are being tracked.

b) In order for information to be provided in an understandable way, it is necessary to use clear language, allowing users to immediately understand that their activities are being tracked when they browse the web and they may ultimately receive targeted ads. The mere use of the word "advertising" alongside the icon is not enough to inform the user that the ad uses cookies for the purpose of behavioural advertising. The wording should as a minimum include the element of "personalised advertising".

c) The icon can serve as additional information and as a reminder notice *after* the subscriber or user has provided his/her consent for the processing of his/her data for the purpose of behavioural advertising. Thus, the proposed icon approach cannot be used for the provision of prior information, as required under the current legal framework (unless it is combined with a way to obtain the user's consent).

d) The information should be correct and complete, as stated in Article 10 of Directive 95/46/EC. The Article 29 WP would like to recall its Opinion 2/2010, where it is stated that "*Ad network providers and 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"*.

Since the icon in itself and the website www.youronlinechoices.eu do not provide accurate and easily understandable information about the different controllers (advertising networks) and their purposes for the processing, the Code and the website do not meet the requirement set out at the revised e-Privacy Directive.

II.2 User choice over Online Behavioural Advertising (Principle II)

In its Opinion 2/2010, the Article 29 WP stated that "*from the literal wording of Article 5(3): 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 EASA/IAB Code, instead of seeking users consent, claims to provide for a way of exercising "choice". In fact it is a choice to opt out, as it offers the user the possibility to object to having his/her data collected and further processed for OBA.

This "choice" is not consistent with Article 5(3) of the revised e-Privacy Directive, as the data are in fact processed without user's consent and without providing the user with information before the processing takes place. Therefore, adherence to Principle II does not meet the requirement set out at the revised e-Privacy Directive.

- User choice site: www.youronlinechoices.eu

The first practical implementation of the EASA/IAB Code is the www.youronlinechoices.eu website, where the method selected to express "choice" is based on the use of different "opt-out" cookies. With the help of such a cookie an advertising network may record the user's refusal to further take part in online behavioural advertising. This approach could easily be modified to be compliant with the amended Article 5(3) of the directive by creating an "opt-in" cookie solution, as explained later on.

The website contains a list with different names of advertising networks. Users may indicate their preference if they do not wish to receive targeted advertising from one, more or all of the networks. Selecting one or more advertising networks results in the installation of one or more opt-out cookies from these networks.

This implementation, apart from the fact that it follows an opt-out approach and thus is not consistent with the requirement for prior informed consent as set out in article 5(3) of the revised e-Privacy Directive, has the following additional problems:

a) Although the opt-out cookie prevents the further reception of personalised advertising, it does not stop the advertising network from accessing and storing information in the user's terminal. On the contrary, it has been demonstrated that an ongoing technical exchange of information between the user's terminal equipment and the advertising network is still in place after the installation of the opt-out cookie.
b) The user is not informed on whether or not the tracking cookie remains stored in his/her computer and for what purpose[5].
c) The installation of the opt-out cookie does not offer the possibility to manage and delete previously installed tracking cookies, whereas at the same time it creates the mistaken presumption that opting out disables the tracking of internet behaviour.

[5] "If you choose to turn off online behavioural advertising it does not mean you will no longer receive advertising on the internet. However, it does mean that the display advertising you see on websites may not be tailored to your likely interests or preferences on the web browser you are currently using." Source: http://www.youronlinechoices.com/uk/your-ad-choices

This problem is worsened by the fact that the website www.youronlinechoices.eu itself contains links to a number of JavaScript functions that are able to track an individual user. This tracking happens without informing the user and, in two cases, without any possibility to opt-out from this specific tracking[6]. Asked to comment on this technical loophole, IAB and EASA have refrained from answering to the Article 29 WP, even after several written reminders.

II.3 Other Principles and areas of concern

II.3.A Sensitive segmentation (Principle IV). Special reference to children

The Code foresees a 12 year age threshold for the processing of children's data. Although this is welcome as a principle, it should be noted that this threshold is not grounded in a legal basis. It would be appropriate to state clearly in the Recommendation that the threshold applies "subject to different mandatory requirements set forth in domestic law".

The Article 29 WP welcomes Part B of Principle IV, which dictates that a user's explicit consent is required prior to creating or targeting OBA segments which make use of sensitive personal data.

II.3.B Compliance and enforcement (Principle VI)

The EASA/IAB Code includes measures for ensuring compliance of the signatory companies to its provisions, especially via the self-certification process which is subject to independent audit and complemented by a periodically renewable compliance "seal". The Article 29 WP recognises the need for internal industry compliance rules, but would like to stress the fact that the Code should in principle comply with the European legislative framework on data protection. In this context, it should be pointed out that it is the national regulators that are ultimately responsible for assessing legal compliance of the OBA providers and performing the relevant enforcement actions.

II.3.C Retention period of collected data

As already explained in Opinion 2/2010, *"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)"*. Furthermore, the collection and processing of data for behavioural advertising purposes must be kept to a minimum. The EASA/IAB Code does not contain any provisions on the amount of data collected and the retention period(s) for the specific purposes. Since the website currently also fails to provide any explanation on this matter, it is unclear how many data are collected by the different advertising

[6] The website contains Java Script functions from five different external third parties. These scripts can collect user information such as IP address, referrer and unique browser configuration.

networks, how long they are stored, and for what purposes they are being processed. This information is absolutely necessary for a user to make a fully informed decision to consent to such profiling. In general, given the lack of transparency and public awareness, it is highly undesirable for each advertising network to have a different retention policy in this regard and a self-regulatory initiative would have been very helpful. Such an initiative should at least address the period in which consent can be considered valid, and after which data shall then be deleted.

III. Some clarifications regarding cookies and consent

III.1 Behavioural advertising involves the processing of personal data

In some parts of the website www.youronlinechoices.eu it stated that *"…in most cases the information used for providing you with these adverts is not personal, in that it does not identify you…"*, and also that a cookie stores *"some basic, non-personal information on your PC to improve certain functionalities and customize the surfing experience"*. These arguments are used to conclude that the installation of cookies for the provision of behavioural advertising is not subject to the data protection legislation. The Article 29 WP refers to its Opinion 2/2010 which outlines that behavioural advertising involves the processing of unique identifiers be that achieved through the use of cookies, or any kind of device fingerprinting. The use of such unique identifiers allows for the tracking of users of a specific computer even when IP addresses are deleted or anonymised. In other words, such unique identifiers enable data subjects to be "singled out" for the purpose of tracking user behaviour while browsing on different websites and thus qualify as personal data.

Moreover, the Article 29 WP would like to note that the Article 5(3) of the revised e-Privacy Directive is applicable independently of whether the information stored or accessed in the user's terminal equipment consists personal data or not. !

III.2 Consent is not required for every type of cookie

The EASA and IAB have also argued that the installation of each single cookie requires "explicit" consent and thus will negatively impact on the surfing experience. The Article 29 WP would like to clarify that consent is not required for every type of cookie, as there are different ways to use cookies with different purposes and requirements associated with them. According to Article 5(3) of the revised e-Privacy Directive, a cookie may be exempted from informed consent if it is "*necessary to carry out the transmission of an electronic communications network*" or if "*it is strictly necessary in order to provide an information society service explicitly requested by the subscriber or user to provide that service*".

As an example, the following cookies would be exempted from informed consent:

- *A secure login session cookie.* This type of cookie is designed to identify the user once he/she has logged-in to an information society service[7] and is necessary to recognize him/her, maintaining the consistency of the communication with the server over the communication network.

- *A shopping basket cookie.* On a shopping website, this type of cookie is typically used to store the reference of items the user has selected by clicking on a button (e.g. "add to my shopping cart"). This cookie is thus necessary to provide an information society service explicitly requested by the user.

- *Security cookies.* Cookies which provide security that are essential to comply with the security requirements of Directive 95/46/EC or other legislation for an information society service explicitly requested by the user. For example, a cookie may be used to store a unique identifier to allow the information society service to provide additional assurance in the recognition of returning users. Attempted logins from previously unseen devices could prompt for additional security questions.

The Article 29 WP further notes that although some cookies may be exempted from the informed consent required by Article 5(3) of the e-Privacy Directive, they may still be used as part of a data processing that must comply with the general data protection directive. In particular, providers of information society services still have to comply with the obligation to inform users. There is sufficient opportunity to inform users about the usage of cookies prior to their setting.

III.3 A pop up is not the only possible way to receive consent

Many people are led to believe that pop up screens are the only way to obtain consent. This is not the case. There are many examples of other, more user friendly ways, to obtain consent. Some of these examples are:

- *A static information banner on top of a website requesting the user's consent to set some cookies, with a hyperlink to a privacy statement with a more detailed explanation about the different controllers and the purposes of the processing.* Such a banner is currently employed by the UK data protection authority[8].

- *A splash screen on entering the website explaining what cookies will be set by what parties if the user consents.* Such splash screens are being used by for example breweries that wish to ensure their visitors are old enough to be allowed to visit the website.

---

[7] An "information society service" is defined as any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service.

[8] http://www.ico.gov.uk

- *A default setting prohibiting the transfer of data to external parties, requiring a user click to indicate consent for tracking purposes.* A practical technical solution[9] has been developed by the German e-zine Heise with regard to cookies set and read by Facebook with the help of its 'Like' button. By default, the button is light-grey. Only if the user clicks on the button, it will be highlighted and become able to set and receive user data[10].

- *A default setting in browsers that would prevent the collection of behavioural data (Do not collect).* Recital 66 of the amended e-Privacy Directive suggests browser settings as a way to obtain consent, provided that they are "*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.

As a minimum, this means that to meet the requirements of Directive 95/46/EC, 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. ! In order for browsers or any other application to be able to deliver valid and effective consent, they must 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. To that end, one might envisage that specific software applications (browser plug-ins or extensions) could be developed by ad networks and downloaded and installed by users to enable changing the status of browser settings with regard to advertising-related cookies by means of application programming interfaces (API) or other tools made available by browser manufacturers. Users should receive the relevant information on data processing as a preliminary step to installing the specific "advertising" plug-in. One might argue that a prerequisite for this opt-in mechanism to work appropriately consists in ensuring that third-party cookies are not accepted by default in browser settings.

The Article 29 WP welcomes recent initiatives by browser providers to develop privacy solutions such as Do Not Track[11] , which could pave the way for compliant consent mechanisms based on browser settings, on the condition that such mechanisms truly enable users to express their consent on a case by case basis, without being tracked by default.

III.4 Clicking through multiple consent "pop-ups" is not always necessary

Since many webpages include cookies from ad networks that would require consent under Article 5(3), EASA and IAB have asserted that users will have to click through consent requests continuously as they go from one website to another. This suggestion does not take into account the fact that once a user has expressed his/her consent or refusal then there is no need to ask him/her again for consent for a cookie serving the same purpose and originating from the same provider. Hence, if a third party ad network

[9] This solution must be accompanied by appropriate information to provide for informed consent.

[10] The specific code is available at http://www.heise.de/ct/artikel/2-Klicks-fuer-mehr-Datenschutz-1333879.html

[11] http://www.w3.org/2011/tracking-protection/

on a website receives consent for an OBA cookie, this consent will not only be valid on other pages of the same website, but also for other websites that share the same OBA network. Consequently, for an average user, the number of consent requests will decrease as he/she navigates and expresses his/her choices.

Once the user has consented to receiving a specific cookie, the presence of the cookie can be used as a marker of such consent. As such, the current "opt-out" technology used by the advertising networks affiliated with the website www.youronlinechoices.eu could be reengineered to provide an "opt-in" approach. As an illustrative example, we can image the following scheme:

1) The first time a user comes in contact with an OBA provider (through a website visit), no cookie has been set, and thus no cookie will be sent to the ad network provider. The ad provider can display a message in any type of information area (including the area where the advertisement would appear) to propose a choice to the user:
   - Accept an "opt-in" cookie for the purpose of future behavioural advertising.
   - Refuse cookies for the purpose of behavioural advertising at the same time accepting a cookie containing the word "REFUSE" so that this refusal can be recorded going forward[12].
   - Store no cookie at all. In that case, the user will be asked again about his choice during the next visit.

2) When the user comes in contact with the same OBA provider again, the ad provider could adjust its behaviour according to 3 possible scenarios:
   - If there is an "opt-in" cookie, the OBA provider can access and store cookies on the user's terminal and provide behavioural advertising.
   - If there is a "REFUSE" cookie, the OBA provider will know that the user refuses future cookies (and thus behavioural advertising), and will stick to untargeted ads.
   - If there is no cookie at all, the OBA provider will consider that this is the user's first contact with him and will ask him about his choice.

This suggestion for a method to obtain consent may be worthwhile to be explored further by the relevant market parties.

Finally, the www.youronlinechoice.eu website demonstrates clearly that choices related to OBA can be presented in a single page where the user can click to express his choices for each OBA provider individually. When a website uses several ad providers, a similar presentation is possible to group together all necessary consent requests to the user in one single page or information area, further reducing the necessary number of "pop-ups" or "information areas".

[12] The use of a cookie to record the user's "refusal" is compatible with Article 5(3), since the user is asked about his consent for that cookie as well.

IV. CONCLUSIONS

As stated in its Opinion 2/2010, the Article 29 WP does not question the economic benefits that behavioural advertising may bring, but it firmly believes that such practices must not be carried out at the expense of individuals' rights to privacy and data protection. The EU data protection regulatory framework sets forth specific safeguards which must be respected.

Adherence to the EASA/IAB Code on online behavioural advertising and participation in the website www.youronlinechoices.eu does not result in compliance with the current e-Privacy Directive. Moreover, the Code and the website create the wrong presumption that it is possible to choose not be tracked while surfing the Web. This wrong presumption can be damaging to users but also to the industry if they believe that by applying the Code they meet the requirements of the Directive.

The advertising industry needs to comply with the precise requirements of the e-Privacy Directive and this opinion shows that many practical solutions are available to ensure a good level of compliance together with a good user experience.

Done at Brussels, on 8 December 2011

For the Working Party
The Chairman
Jacob KOHNSTAMM