# I (do not) consent to behavioural advertising

By Evangelia Mesaikou

## 1. Introduction

During the last years, the online advertising industry has developed new techniques in order to maximize its benefits by providing more targeted advertisements to internet users according to their interests. By placing cookies or other tracking devices into the users' terminal equipment, advertisers collect data and create a profile for each user based on the web pages visited and the searches made and then provide tailor made advertisements. For example, online advertisers may know or assume your gender, where you live, where your next vacation is planned and even more intimate details, such as if you are trying to lose weight, if you have medical disorders, and they use that information to provide you with advertisements that might interest you. This is called behavioural advertising and it is considered to be the most effective way of online advertising. This is because it helps advertisers to reduce the amount of advertisements shown (and consequently their cost) only to a target of users and at the same time increase the percentage of responses to their advertisements. Internet users can also benefit from behavioural advertising because they will not receive many irrelevant advertisements and they might get to know products that they are interested in (Petty Ross 2000).

However, online behavioural advertising raises some important data protection issues. The most significant problem is that most internet users are not aware that third parties, and not only the sites they visit, install tracking devices to their terminal equipments and can trace their activities and compile profiles for them. In other words, they are not informed who has access to which data and for how long in order to consent or not to this processing.

Since tracking devices are installed in the terminal equipment of the internet user (data subject), and sites access this information in order to process data and build up a profile for the individual, the European framework of data protection legislation is applicable (Directive 95/46/EC and Directive 2002/58/EC, so called e-Privacy Directive). Under these legislations, the advertising network providers and the publishers of the advertisements have specific obligations and the data subjects should be granted with specific rights.

Due to the recent amendment of the e-Privacy Directive, which has to be implemented into the national laws of the Member States until 25/05/2011, the lawfulness of behavioural advertising has become a flaming issue for academics, regulators and industry. This is because, under the amended version of Article 5(3) of the e-Privacy Directive the informed and freely given consent of the data subject is a prerequisite for the data processing in order for online behavioural advertising to be lawful. Online

behavioural advertising is also at the top of the agenda in the US, where Representative Jackie Speier (D-California) recently introduced the "Do Not Track Me Online" Act, which calls on the Federal Trade Commission (FTC) to issue regulations requiring that Web companies allow consumers to opt out of online tracking; in addition, Representative Bobby Rush (Illinois) reintroduced an online privacy bill that would require ad networks to obtain users' consent to tracking. As a response to these regulatory changes, the online advertising industry is trying to come up with solutions (mainly through self regulation or privacy by design schemes) in order to be compliant with the law without having to restrict the profitable business of targeted advertisements.

This paper is structured as following. The legal requirement of consent to behavioural advertising under the amended version of Article 5(3) of the e-Privacy Directive is further analyzed in section 2. Moreover, possible solutions which are proposed in the EU and the US in order to address these data protection concerns are examined in section 3, and in particular the default browsers settings, the do not track lists, the use of a warning icon and the feasibility of opt in mechanisms. Finally, the conclusion of this paper is that a balance should be found in order not to overly restrict behavioural advertising business but at the same time protect the privacy and data protection rights of the internet users. From this perspective, my recommendation is that the default privacy settings should change in order to require affirmative action of the user to consent to being tracked for commercial purposes and in addition a layered approach might be the most effective mechanism to provide the users with notice and choice.

## 2. Legal requirement of consent to behavioural advertising

In order to examine the data protection issues raised in online behavioural advertising, we should understand how it works, the factors involved and the methods used. In online behavioural advertising there are three different roles: the advertising network providers (also referred to as "ad network providers"), the advertisers and the publishers. The ad network providers are the most important factors since they are the ones that connect the advertisers with the publishers. In other words, their role is to display advertisements of their associated advertisers on the specific space reserved for this reason in the publishers' web pages. In order to be more effective and display the most interesting advertisements to each user, they use tracking methods so as to identify each internet user as a unique user, collect information for him while the user is browsing online and compile his profile (Article 29 Data Protection Working Party, 2010). As the network of ad network providers can include hundreds of different web pages, the ad network providers collect a lot of information for each user and can compile a rich profile about his activities and interests.

The main tracking method for the purposes of online behavioural advertising is the use of cookies. Other methods, less common and more pervasive while some even illegal, are the use of data mining software and spyware, but these are out of the scope of this paper. Cookies are piece of data that a webpage sends to a web browser, along with a request that the user's web browser retains it. The cookies used in the above scheme of behavioural advertising are third party cookies, because they are placed from a third party (the ad network provider) into the user's browser when the user is

visiting a webpage (of a publisher) that contains content from this third party (ad network) provider. Lately, online advertising companies have started using more persistent types of cookies in order to improve their services, such as super cookies and Flash cookies. These are "stronger" cookies because they use mechanisms which are able to store in more persistent way users' identifiers, sometimes recover deleted cookies and they cannot be deleted through the traditional settings of a browsers (ENISA, 2011).

According to ENISA's Report, *"some studies showed that the penetration of the top 10 third-parties grew from 40% in 2005 to 70% in 2008, and to over 70% in September 2009. Another study shows that not only are these third-parties increasing their tracking of users, but that they can now link these traces with identities and personal information via online social networks"*. The protection of users' equipment against this increasing penetration by third parties should be an objective itself. Article 5(3) of the e-Privacy Directive is applicable because of the fact of the penetration to the user's equipment, meaning the use of cookies, regardless if the data processed constitute personal data under the meaning of Directive 95/46/EC. Apart from that, depending on the circumstances and the nature of the processing executed by this penetration, as well as the types of data processed from the users' equipment, the Directive 95/46/EC may apply to such processing. The latter is fully applicable except for the provisions that are specifically addressed in the e-Privacy Directive (Article Article 29 Data Protection Working Party, 2010). Therefore, the principles of data quality, technical and organizational security measures, data retention period, the rights of the data subjects and the protection of sensitive data should be respected as well. For the purpose of this paper, we will focus on the requirement to obtain the users' consent under the amended version of Article 5(3) of the e-Privacy Directive.

Article 5(3) reads as following: *"Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service."* Therefore, Article 5(3) applies to HTTP cookies, Flash cookies and any similar devices which may perform the functions described in the provision (EC, Information Society and Media DG, 2010). According to this Article, cookies that are not strictly necessary for the provision of the service requested by the user may only be used if the user has given his freely and informed consent in advance. Under this exception usually fall first party cookies, which are cookies sent by the webpage visited by the user in order to "remember" the preferences of the user, such as the language settings, purchase list, or username and password. However, online behavioural advertising cannot fall under this exception. Even if someone would argue that internet is flourishing and there are many online services free of charge because they are financed by advertisements, therefore, behavioural advertising, as the most profitable way of online advertising, is necessary for the provision of online services and therefore it should fall under this exception, this is not a correct argument. The exception that is covered by the above Article is only for "strictly

necessary" processing in order to provide a service explicitly requested by the user, and thus behavioural advertising cannot be considered as such and the prior consent of the user is required (EuroPriSe, 2010).

In order for consent to be valid, it should be informed and freely given before the placement of the cookie. The users should be provided with all the relevant information about the cookie and the processing, which should include the identity of the controller, the recipients of the data, the purposes of the processing and any disclosure to third parties. This information must be provided in a user friendly way, so as to be easy for the average internet user to understand to what he is about to consent. The user should have the choice to accept or refuse the placement of the cookie and moreover consent should be revocable. This means that any time the user would like to change the settings and revoke his consent about such processing, it should be easy to do it and his choice must be respected. Moreover, consent must be specific, which means that any change in the purposes of the processing after the user's consent was given is not covered by this consent (EC, Information Society and Media DG, 2010).

The responsibility to provide such information to the internet user lies with the entity which sends the cookies and retrieves information from the cookies stored on the terminal equipment of the user, thus most commonly the ad network providers. In some cases when publishers are joint-controllers with ad network providers, for example when they transfer directly identifiable information to ad network providers, they are obliged to provide information to users about the data processing (Article 29 Data Protection Working Party, 2010). Therefore, collaboration is needed between ad network providers and publishers to provide in a user friendly way and in understandable language the necessary information to the users. Moreover, since users usually ignore that third parties might send them cookies when they visit a publisher's webpage, publishers are responsible to inform them (in a user friendly way of course and not in between the long list of terms and conditions of their webpage) that they "rent" place to ad network providers to display advertisements and warn them that these third parties might send cookies to them.

After this short analysis, it is obvious that under the amended version of Article 5(3) of the e-Privacy Directive, the prior informed consent is required before a cookie is sent to the user's terminal equipment and therefore in order from online behavioural advertising to be lawful, the ad network providers should obtain in advance the consent of the internet users to be tracked for the purposes of advertising. Any company operating in the EU market or any online product that is targeted at EU consumers must comply with this rule. This might constitute a problem for many companies after May 25$^{th}$ 2011, which is the deadline for the implementation of the amended e-Privacy Directive into national laws. In the next section the different solutions proposed by industry and regulators to address this issue are presented.

## 3. Technical solutions to obtain consent

Currently, online behavioural is taking place based on opt out methods. This means that ad network providers send cookies to internet users' terminal equipments in order

to process their data and provide them with targeted advertisements unless users have opted out from receiving third party cookies. Article 29 Working Party urges publishers and ad networks to move away from opt-out mechanisms and create prior opt-in mechanisms instead. Users should provide their consent with an affirmative action that shows their "willingness to receive cookies and the subsequent monitoring of their surfing behaviour"; inaction of the users to change their settings does not mean that they consent to be tracked according to the amended Article 5(3) of the e-Privacy Directive. So far, different solutions to address this issue were proposed and some of them are already implemented through self regulation from some companies. Below is a short analysis of the main mechanisms proposed.

Default settings of internet browsers

At present, the default settings of web browsers are set to accept first and third party cookies and they give the choice to the internet user to change these default settings and choose either to opt-out from receiving third party cookies or to be asked for permission before a cookie is sent to his terminal equipment. Under the new requirement of prior consent, the current default settings of the browsers are not sufficient anymore because the user's consent cannot be implied if the user does not change his browser's settings. Most of the users are unaware that not only the sites they visit but also third parties install cookies to their terminal equipment in order to process certain data and usually they also do not know how to change their browser's settings (Article 29 Data Protection Working Party, 2010).

Therefore, the current default settings of the browsers are not compliant with the legal requirement of prior consent. If the default settings would be not to accept third party cookies which would require ad network providers to obtain the user's consent before the placement of each cookie most probably with a pop up window, it would be compliant with the law but this would not be a user friendly solution. Imagine while a user is surfing online a pop up window to appear almost each time the user is visiting a different webpage informing about the cookies and requiring user's consent. Probably this would have the exact opposite results, by annoying the user who would click "accept" to everything without reading the provided information, just to make the procedure faster and get rid of the pop up window. In addition, it seems that under this setting, users would still be tracked through Flash cookies or other mechanisms.

It seems that the presented solution of browsers' settings is a very unconditional solution, since it offers to the user the choice either to receive all third party cookies or opt out in total (Berger, 2010). Even if the browsers implement this change into the new versions they release, practically it might take many years for browsers with the old default settings that have not been updated to be phased out, thus rendering ad network providers non-compliant in relation to those outdated browsers in the meantime. Therefore, collaboration with browsers and ad network providers is needed in order to find a more suitable solution, which could consist in a combination of default browsers' settings not receiving third party cookies with a good mechanism in place for ad network providers to obtain consent in order to provide their services to the users. For such mechanism, a layered approach could be a promising solution and this is further analyzed in the conclusions and recommendation section.

Do not track lists

The solution which is more favourable in the US is the implementation of a mechanism so called "Do not track" lists. The Federal Trade Commission (FTC) in its preliminary staff report issued in December 2010, proposed a new privacy framework and suggested the implementation of do not track lists in order to promote self regulation in online behavioural advertising. However, the FTC has not endorsed any Do not track mechanism yet. As a result, it is not clear exactly how this could be implemented, but the most practical method of providing a browser based mechanism would likely consist in placing a setting similar to a persistent cookie on the user's browser which would convey that setting to the web pages visited to signal whether or not the consumer wants to be tracked or receive targeted advertisements (FTC Staff Report, 2010).

After the release of the FTC Report, the industry has taken the initiative to develop and even implement such mechanisms through self regulation. Both Microsoft and Mozilla released new versions of their browsers (Internet Explorer 9 and Firefox 4 respectively) which support a Do Not Track mechanism. This mechanism is inactive at the default settings of the browsers and the user has to add a list or lists made by organisations or customise his own do not track list. Such list contains web addresses that the browser will visit/call only if the user visits them directly by clicking on a link or typing their address. By limiting the "calls" to these websites and resources from other web pages, the lists limit the information these other sites can collect. At the moment, ad network providers don't have any legal obligation to abide by these users' stated preferences, but it's a bit of an honour system and the effectiveness of such mechanism is not yet tested.

Under the requirement of prior opt–in consent set by Article 5(3) of the e-Privacy Directive, the current implementation of such mechanism would not be adequate in the EU, since it is inactive as a default browser setting. Moreover, its effectiveness is to be tested, and also a clear definition of what the notion "tracking" includes is needed. If all the tracking methods are banned by the "do not track" mechanism and if this is active in the default browsers' settings, then it might turn to be more effective than the blocking solely of third party cookies.

Warning Icon

In the US TRUSTe, an internet privacy services provider, has launched a pilot program, called Behavioural Advertising Notice and Choice Program, based on the FTC and industry coalition self-regulatory guidelines for behavioural advertising. Publishers who participate in this pilot program will display the TRUSTe icon and a message (such as "Your Info and Ads") on their web pages where behavioural advertising takes place. When the user will click on this icon a pop-up widget will open providing users with a short notice about the advertisements appearing on the site, the available choices to opt-out and the ability to leave feedback or file a complaint. The pilot will test icon placement, alternative notice and choice messaging and consumer engagement levels. Yahoo and Google are participating in this program and they have started using this TRUSTe icon. These companies link the ad icons to tools allowing users to change the categories of interests of their associated companies

and to opt out from receiving behaviourally advertisements. The large online services companies (i.e. Google, Yahoo, Microsoft, AOL) have decided to use the same icon in order to have a united approach and make it easier for the user to recognize it and understand its use. The icon proposed by TRUSTe is the following:

The use of warning icon is also supported in the EU, such as in the European Advertising Standards Alliance Report (2010), in order to provide in a user friendly way notice to the users about behavioural advertising.

The industry can conduct surveys in order to find the most effective icon and messages icon to attract consumers' attention, without misleading them. Such a survey (Hastak and Culnan, 2010) showed that messages such as *"Why did I get this ad?"* and *"Interest based ads"* had greater interaction with the users than *"Sponsor ads"* or *"Adchoice"*. It would be important as well to adopt the same or a similar icon, in order to make it easier for the user to recognise it and understand its role. In order this approach to bring fruits, consumer education will be needed to improve the effectiveness of the communication adopted by the ad network providers over time.

Feasibility of opt-in mechanism

Another proposal is a universal choice mechanism which would give the users the choice to opt out from being tracked and offered targeted advertisements completely as well as the choice to see the categories of advertising associated with them, de-select some categories and/or select additional ones. Under this approach users would be able to choose what type of advertisements they are interested to receive or whether they do not want to receive targeted advertisements at all.

The feasibility of such mechanism in a universal basis is not yet confirmed by industry. However, some companies, such as Google, already have in place a similar mechanism for their associated companies. Under this mechanism, so called Ad Preference Managements, the user get notice of which of the more or less 20 categories and 600 subcategories have been associated with the tracking cookie in the user's browser and it gives him the choice to specify which categories he is really interested in or opt-out completely from having his data collected for the purposes of online behavioural advertising (Szoka, 2009). A similar mechanism is used by Yahoo as well.

Such universal mechanism would facilitate the user since he would give his choices in "one-shop stop" and not in each company's ad preference mechanism. However, it

raises some other issues apart from consent, such as data access and data retention period, security etc. Moreover, since the user's consent needs to be specific, it is doubtful whether consent for tracking for specific categories in such universal mechanism would be sufficient for the processing of data by different companies based on this consent.

## Conclusion and recommendations

As it was analysed before, online behavioural advertising is a very effective way of advertising and a very profitable business. According to the Interactive Advertising Bureau's Report conducted by the PricewaterhouseCoopers LLP (2010), *"Internet advertising revenue in the U.S. totalled $6.2 billion in the second quarter of 2010, an increase of 4.1 percent from the 2010 first quarter ... and an increase of 13.9 percent from the 2009 second-quarter ... Year-to-date Internet advertising revenues through June 2010 totalled $12.1 billion, up 11.3 percent from the $10.9 billion reported for the same six-month period in 2009."* However, according to another report conducted by the Ponemon Institute (2010), the online advertising industry is seriously concerned about the data protection issues raised and this has a potential impact on this industry. The survey conducted showed that for their benchmark sample, the average lost potential spending on online behavioural advertising amounts to 6.72$ million, and the average opportunity loss resulting from privacy concerns is 30.69$ million.

On the other hand, despite the benefits that online behavioural advertising has for the advertising industry and also for the consumers, the tracking of the consumers/users is taking place most of the times without their knowledge and consent. Internet users ignore the fact that third parties send cookies and track their online behaviour in order to provide them with tailor made advertisements. They think that what they do online is private and they behave accordingly, for example they tend to type in search engines very intimate queries even for their medical problems. An empirical study on how users perceive behavioural advertising showed that 64% of the sample finds the idea of behavioural advertising invasive and that only 51% believes that behavioural advertising is happening a lot now (McDonald and Cranor, 2010).

Therefore, online behavioural advertising needs to change. Under the amended e-Privacy directive, the ad network providers need to adopt another change, which is the requirement to obtain the prior informed consent of the user before the placement of the cookies to his terminal equipment, as analyzed in section 2. Member States have to implement this Directive into national law until 25/05/2011; however, regulators and business seem to be quite unprepared for this change. There are no recommendations about the implementation of the Directive into national law issued by any Data Protection Authority to date and at the same time the discussion about technical solutions from the business are still ongoing.

Recognizing that online advertising plays an important role in financing free online services and in fostering internet innovation, it is understandable that a balance should be found between these conflicting interests of behavioural targeting users and respecting users' privacy and data protection rights. It is very important to find and

implement potential solutions to protect users' rights, without going too far and as a result overly restrict the behavioural advertising industry. Since, online behavioural tracking and advertising should not take place without the user's consent, business should develop user friendly opt in mechanisms. At the moment, a layered approach seems to be the most promising solution and such a scheme is shortly presented below.

A layered approach should first of all have different default browsers' settings. Under these default browsers' settings either third party cookies will be rejected unless the user adds specific exceptions or a "do not track" list will be activated (if its effectiveness and adequacy is tested). Consequently the users will not be tracked and offered behavioural advertisements anymore without their knowledge and consent. Needless to say that the users will still be provided with advertisements, but not based on tailor made based on profiles compiled for them through tracking. Secondly, the online advertising industry should come up with innovative, user friendly mechanisms to obtain user's consent. It is advisable not to have too many different mechanisms in order not to confuse the users. Such mechanisms could be the use of a marketing message at a part of the place reserved on the web pages of the publishers for advertisements, inviting the users to visit the webpage of the ad network provider, where there would be information about online behavioural advertising as well as the information about the data controller and the tracking practices of this ad network provider. The user would be offered the option to consent to be tracked for behavioural advertising by this ad network provider and possibly also to choose some categories he would like to receive advertisements for. Therefore education of the users is needed in order to understand better how internet and the online advertising industry are working. Finally, besides that, each time a behavioural advertisement is shown to the user, the use of the warning icon of behavioural advertising, such as the one proposed by TRUSTe, could be displayed on the advertisement, in order to provide information to the user why this advertisement is shown to him and give him the chance to revoke his consent.

Even if the industry seems reluctant to give up the current opt-out mechanisms on which online behavioural advertising is based now, the law in Europe has changed and industry needs to keep up with this change and bring innovative solutions in order to be lawful and at the same time keep the benefits of behavioural advertising. There is a need for greater transparency and better user notice and choice opt- in mechanisms.

**List of References**


Article 29 Data Protection Working Party (2010), Opinion 2/2010 on online behavioural advertising, online at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf /accessed 31.03.2011

Berger, D. (2010), Balancing consumer privacy with behavioural targeting, online at http://ssrn.com/abstract=1693029 /accessed 31.03.2011

ENISA (2011), Bittersweet cookies. Some security and privacy considerations, online at http://www.enisa.europa.eu/act/it/library/pp/cookies/ accessed 31.03.2011

European Commission (EC), Information Society and Media DG (2010), Working Document with subject: Implementation of the revised Framework– Article 5(3) of the ePrivacy Directive, online at: http://itek.di.dk/SiteCollectionDocuments/Blandet/Sikkerhedsnyhedsbrev/COCOM10-34%20Guidance%20Art%205%283%29%20eprivacy%20Dir.pdf/ accessed 31/03/2011

EuroPrise (2010), Position paper on the impact of the new "Cookie Law" on certifiability of behavioural advertising systems according to EuroPriSe, online at: https://www.european-privacy-seal.eu/results/Position-Papers/PDF%20-%20EuroPriSe%20position%20paper%20on%20the%20new%20cookie%20law.pdf/ accessed 31/03/2011

FTC Staff Report (2010), Protecting consumer privacy in an era of rapid change, online at: http://www.ftc.gov/os/2010/12/101201privacyreport.pdf/accessed 31/03/2011

Hastak, M., and Culnan, M. (2010), Online Behavioral Advertising "Icon" Study, online at: http://futureofprivacy.org/final_report.pdf

McDonald, A. and Cranor, L. (2010), Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising, online at: http://www.aleecia.com/authors-drafts/tprc-behav-AV.pdf / accessed 31/03/2011

Petty, Ross D. (2000), "Marketing Without Consent: Consumer Choice and Costs, Privacy, and Public Policy." Journal of Public Policy & Marketing 19, no. 1: 42-53

Ponemon Institute LLC (2010), Economic impact of privacy on online behavioral advertising. Benchmark study of Internet marketers and advertisers, online at: http://www.evidon.com/documents/OBA_paper.pdf / accessed 31/03/2011

PricewaterhouseCoopers LLP (2010), IAB Internet Advertising Revenue Report, online at: http://www.iab.net/media/file/IAB_report_1H_2010_Final.pdf/ accessed 31/03/2011

Szoka B. (2009), Google's Ad Preference Manager: One Small Step for Google, One Giant Leap for Privacy. The Progress & Freedom of Foundation, volume 5 issue 2, available online at: http://ssrn.com/abstract=1421876/ accessed 31/03/2011