ARTICLE 29 Data Protection Working Party

Brussels, 3 August 2011

OBA Industry

IAB (Interactive Advertising Bureau) Europe
Ave Livingstone 26
1050 Brussels

EASA
(European Advertising Standards Alliance)
Rue de la Pépinière 10-10a
1000 Brussels

Dear Madam, Sir,

As agreed a meeting has been scheduled in order to discuss the self-regulatory Framework for Online Behavioral Advertising as presented by the Internet Advertising Bureau Europe (IAB Europe) and the European Advertising Standards Alliance (EASA), referred to as the Best Practice Recommendation on Online Behavioral Advertising (hereinafter the EASA/IAB Code).

As this meeting could only be scheduled in September, I would like to inform you in advance of the main concerns the Article 29 Data Protection Working Party has with the EASA/IAB Code at this stage, specifically relating to the requirement of informed consent pursuant to the ePrivacy Directive. Please find these main concerns outlined in Annex I.

Please also find attached a letter received from the United States' Federal Trade Commission for your information, Annex II.

I look forward to discussing these and other issues further with you in September.

Yours sincerely,
On behalf of the Article 29 Working Party,

Jacob Kohnstamm
Chairman

Cc: Commissioner Kroes, Mr. Robert Madelin, DG INFSO,
Mrs. Francoise Le Bail, DG Justice

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No LX-46 01/190.

Website: http://ec.europa.eu/justice/policies/privacy/index_en.htm

Annex I

Primary data protection concerns with regard to the EASA/IAB Code

The revised ePrivacy Directive requires user consent to place cookies on their terminal equipment and to further access them. Article 5(3) requires consent to be obtained after the users have been provided with clear and comprehensive information. The criteria to determine whether consent is valid are the same as those set forth in Directive 95/46/EC. In accordance with Article 2(h) of that Directive, for consent to be valid, it must be *freely given, specific and informed. It must also be an indication of the data subjects wishes.* In practice, in the context of online behavioral advertising, this means that to obtain consent, ad network providers must provide the necessary information before the cookie is sent and rely on users' actions (e.g. clicking a box stating "I accept") to signify their agreement to receive the cookie and to be tracked for the purposes of serving behavioral ads.

The need for a clear indication of the user's wishes

The mechanisms proposed by the EASA/IAB Code enable people to object to being tracked for the purposes of serving behavioral advertising. However, tracking and serving ads takes place unless people exercise the objection. While this mechanism is welcome and constitutes an improvement to the current situation, it does not meet the requirement to obtain the aforementioned informed consent. For such mechanism to be a valid form of consent, it should leave no doubt about the users wishes. It can not be concluded that users who have not objected to being tracked for purposes of serving behavioral advertising have exercised a real choice. In other words, if an individual has not given an indication of his wishes, such absence of action cannot be presumed to indicate his consent. This is even more so if the relatively limited knowledge users have about online behavioral advertising and the procedures to object is taken into account. Therefore the Working Party 29 considers that the proposed mechanisms would lead to consent of many Internet users being wrongly assumed. Online behavioral advertising will therefore rely on consent that is, in fact, illusory.

Need for streamlined procedures for multiple ad network providers

Industry has indicated that, given the number of ad network providers that may be present on a given website (because the website operator has contracts with multiple ad network providers), mechanisms that would require the users to indicate their consent would entail multiple pop-ups.

The Working Party notes that as each ad network provider is a different entity which sends a cookie to the user terminal equipment, each provider engages separately in profiling and the subsequent sending of targeted ads. Thus, the legal provisions apply to each ad network provider. Furthermore, the Working Party considers that users should not be deprived of their statutory right to decide to receive cookies (or not) simply because the website operator has contracts with multiple ad network providers.

The Working Party would like to recall that consent is not required for each individual cookie access or transmission by a website: once the user has agreed to let a specific ad network transmit and access specific cookies on his terminal, this ad provider does not need to ask the

user again for subsequent access and transmissions of cookies serving the same purpose (though the ability to 'opt-out' should be available). When the user arrives on a new website, it is thus possible that he will already have expressed his wishes regarding some (or even all) of the cookies distributed by ad networks present on that website. Consequently, the potential number of pop-ups will naturally decline as the user navigates on the Net.

Additionally, the Working Party considers that it should be feasible for web site operators and ad network providers to set up streamlined procedures whereby users could accept (or decline) cookies of the various ad network providers publishing ads on one website, in a centralized way, while respecting granularity. The Working Party encourages all industry-stakeholders to work together towards finding workable solutions.

Browser settings

The Working Party would like to recall that in order to consider consent through browser settings valid, it will have to be "*technically possible and effective, in accordance with the relevant provisions of Directive 95/46*" (recital 66 of the ePrivacy Directive). 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, as long as it is technically possible, effective and in accordance with all relevant requirements for valid consent.

To meet the requirements of the ePrivacy Directive and 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. This is even more so given the relatively limited knowledge of users about browser settings and behavioral advertising. The Working Party considers that, in order for browsers or any other application to be able to 'deliver' valid consent, they must by default reject third party cookies and require the data subject to engage in an affirmative action to accept cookies from specific websites for a specific purpose. Furthermore, in order to meet the requirements of Directive 95/46/EC browsers should convey, on behalf of the ad network providers, the relevant information about the purposes of the cookies and the further processing.

The Working Party realizes that in the last year, browser providers have made important efforts. However, all the solutions presented so far continue relying on default options that accept cookies.

Clear and comprehensive information

Under Article 5(3), consent must be informed. In order for consent to be valid, it must be given after the user has been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, *inter alia,* about the purposes of the processing. In practice, this means that the way in which the information is given is crucial. It must be given in a way that average Internet users will understand it.

Under the EASA/IAB Code, an icon will be used as a notice. In the future, it is possible that the icon might eventually be recognized by average Internet users who, depending on how it is provided, may be able to understand its underlying meaning. However, nowadays an icon will mean very little to users. This means that average users will not be given the legally required information and will not be able to make choices. The Working Party considers that information must be provided using clear and comprehensible language, stating that users'

activities are being tracked when they browse a website and the fact that they are profiled in order to send advertisements. For example, the use of the word "advertising" is not sufficiently clear to be used as a notice to inform individuals that they are being tracked and for which purposes. Furthermore, affirmations in the Code such as *"...in most cases the information used for providing you with these adverts is not personal, in that it does not identify you..."* are likely to be confusing for users insofar as it may lead them to believe that the tracking has no privacy implications for them. Article 5(3) of the ePrivacy Directive is applicable whether there is personal data or not. Furthermore, users are not informed of the profile that is created with their navigation information and associated to a single ID cookie.

The information provided on www.youronlinechoices.com also seems ambiguous when not informing users clearly that they are being tracked across websites and it appears to lack detailed information on the procedure of profiling.

Availability of information

The availability of the information is crucial. Information must be given directly to individuals, it is not enough for information to be available somewhere. This requirement has to be applied alongside with the requirement for information to be clear and comprehensive. As the ePrivacy Directive requires, to store information or to gain access to information stored in the terminal equipment of a subscriber or user, information is supposed to be given directly to individuals in order to let them give their informed consent. Users should not be required to have to search to find the relevant information. However, under the EASA/IAB Code, once the user clicks on the icon, (s)he will still need to click at least two times to obtain the additional information and be able to opt out. Information which is key to trigger a user reaction should be directly visible.

****

ANNEX II

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of the Director
Bureau of Consumer Protection

Mr. Jacob Kohnstamm
Chairman of the Article 29 Working Party
Chairman of the College bescherming persoonsgegevens
Postbus 93374
2509 AJ Den Haag, Netherlands

June 1, 2011

Dear Jacob:

Thank you for your May 30, 2011 letter. I appreciate the opportunity to share the current thinking of the Federal Trade Commission ("FTC") staff on transparency and consumer choice in connection with behavioral advertising.

Online behavioral advertising is the practice of tracking consumers' activities online, including across websites, in order to infer information about their interests and serve them advertisements tailored to those interests. As we have discussed, this practice helps to subsidize and support a diverse range of online content and services that otherwise might not be available, or that consumers would otherwise have to pay for—content and services such as blogging, social networking, and news from around the world. At the same time, of course, behavioral advertising raises consumer protection concerns relating to privacy. Today, many consumers do not even know they are being tracked when they visit Internet sites. Those who do may be uncomfortable with being tracked—particularly if the information is used for purposes other than serving them ads.

For this reason, the FTC staff has advocated for greater transparency and consumer control over behavioral advertising. It has issued two reports that discuss the subject. In its 2009 report on behavioral advertising, the FTC staff supported the idea of "just in time" disclosures as a way of improving transparency of the practice of behavioral advertising.[1] The report noted that a disclosure "that is located in close proximity to an advertisement and links to the pertinent section of a privacy policy explaining how data is collected for purposes of delivering targeted

[1] FTC Staff Report, *Self-Regulatory Principles for Online Behavioral Advertising* (February 2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

advertising, could be an effective way to communicate with consumers."[2] The report also noted that the "just in time" disclosures should link to choices for consumers.[3]

In its 2010 preliminary staff report on consumer privacy,[4] the FTC staff recommended simplifying the presentation of privacy choices to consumers in all contexts. It reiterated support for the concept of "just in time" disclosures to accompany such choices.[5] Although the report did not take a position on whether the choices for consumers should be "opt in" or "opt out" as a general matter, it did state that companies should not collect certain sensitive information—such as health, financial, children's and precise geolocation information—without obtaining consumers' affirmative express ("opt-in") consent.[6] Finally, in the context of simplifying choice for online behavioral advertising, the report called for a universal and effective Do Not Track system.[7] Since the report was issued in December 2010, the FTC has indicated its support for a Do Not Track mechanism in testimony before the U.S. Congress.[8]

Since issuance of these reports, industry has taken a number of steps to improve transparency and consumer choice in the context of behavioral advertising. Several self-regulatory efforts to implement Do Not Track are underway, including an effort by a coalition of online advertising networks, as well as efforts by browser vendors.[9]

---

[2] *Id.* at 35-36.

[3] *Id.* at 35.

[4] FTC Preliminary Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change* (December 2011), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf. We are currently reviewing public comments and expect to issue a final report later this year.

[5] *See, e.g.*, *id.* at 64.

[6] *Id.* at 61.

[7] *Id.* at 66.

[8] *See, e.g.*, Prepared Statement of the Federal Trade Commission On The State of Online Consumer Privacy Before the Committee On Commerce, Science, and Transportation, United States Senate, March 16, 2011, *available at* http://www.ftc.gov/os/testimony/110316consumerprivacysenate.pdf.

[9] *See, e.g.*, Prepared Statement of the Federal Trade Commission On The State of Online Consumer Privacy Before the Committee On Commerce, Science, and Transportation, United States Senate, March 16, 2011, *available at* http://www.ftc.gov/os/testimony/110316consumerprivacysenate.pdf, at 14-16 (describing Digital Advertising Initiative self-regulatory system and efforts by browser vendors to implement Do Not Track and block targeted ads).

As these industry efforts continue, FTC staff has provided guidance on the essential components of a successful Do Not Track mechanism as follows:[10]

- Simplicity: A Do Not Track mechanism must be easy for consumers to use and understand. No Do Not Track mechanism will succeed if consumers cannot figure out how to locate it and use it.

- Effectiveness: An effective Do Not Track mechanism would prevent the tracking of consumers by any means, including traditional http cookies, Flash cookies, or any other technological means. Effectiveness also means that choices are respected. For example, we recently brought a case against a company that offered an opt out of behavioral targeting that—unbeknownst to the consumer—expired after 10 days.[11] Obviously, such a choice is illusory and not effective. Finally, effectiveness includes enforceability; thus, any Do Not Track system must have a robust accountability and enforcement regime.

- Universality: A Do Not Track mechanism needs to be universally honored across companies and industry. Consumers should not have to exercise choices on a company-by-company basis.

- The Choice Should Apply to Tracking and Not Just Advertising: Some consumers may object not just to targeted advertising but to the data collection underlying it, especially if the data could be sold to data brokers, insurance companies, or employers. Thus, a Do Not Track mechanism must allow consumers to opt out of both targeted advertising and tracking for other purposes—provided, of course, that companies should be allowed to collect information on consumers for a limited set of commonly accepted purposes, such as detecting fraud.[12]

- Persistence: An effective Do Not Track mechanism would ensure that consumers' choices will be persistent. Consumers should not have to reset their preferences every time they clear their cookies or close their browsers.

---

[10] *See, e.g.,* Prepared Statement of the Federal Trade Commission On The State of Online Consumer Privacy Before the Committee On Commerce, Science, and Transportation, United States Senate, March 16, 2011, *available at* http://www.ftc.gov/os/testimony/110316consumerprivacysenate.pdf (setting forth elements that an effective Do Not Track mechanism must contain). The testimony noted that the 2010 preliminary staff report did not take a position on whether Do Not Track should be adopted through legislation or self-regulation.

[11] *Chitika, Inc.*, FTC File No. 102 3087 (Mar. 14, 2011) (consent order accepted for public comment).

[12] The specific practices designated by FTC staff as "commonly accepted" are identified in the FTC Staff Privacy Report. *See* FTC Staff Privacy Report, at 54.

I know that there is broad agreement in the EU that transparency and consumer choice in the context of behavioral advertising are essential. As we emphasized in the two staff reports discussed above, FTC staff shares the view that consumers must have clear information about how their data is collected and used and must have a meaningful opportunity to control these practices.

While I am not in a position to comment on the specific EU industry self-regulatory initiative mentioned in your letter, I welcome this opportunity to exchange views. I appreciate your deep commitment to protecting consumers' privacy, and I believe that this kind of international dialogue is essential in today's globalized economy. I look forward to continuing to work closely with you and your colleagues on this and other important privacy issues.

Sincerely,

David C. Vladeck

ANNEX III

ARTICLE 29 Data Protection Working Party

Brussels, 30 May 2011

Mr. David C. Vladeck
Director of the Bureau of Consumer
Protection of the Federal Trade
Commission

United States of America

Dear David,

As you know online behavioural advertising remains a hot topic within the European data protection community. By 25 May 2011, the revised e-privacy directive officially had to be implemented in the national law of the 27 Member States. The legal demand of prior, informed consent has given rise to a public debate in which the core issues are simplified into opt-in versus opt-out.

Recently a self-regulation scheme has been launched by IAB Europe and EASA, which includes the website www.youronlinechoices.com. Although no full assessment of the scheme has (yet) been made by the Article 29 Working Party, I cannot exclude that the plans are not fully in line with the intention of and reasons for the revised legislation. Apparently, the relevant industry claims a large divide between the vision and analysis of the European supervisory authorities and the approach chosen by the FTC. I feel this is unjust, as both WP29 and the FTC share a concern about the lack of transparency of the practice of behavioural advertising. We both see the need to enable effective choice. The key question is 'who has control, the consumer or the advertising industry'?

To align our visions is important in itself, but even more so given today's globalized economy. Therefore I am interested in learning about the FTC staff's views on transparency and consumer choice in connection with online behavioural advertising. I am convinced we can work from there to find common ground and ensure a good protection of consumers' interests on both sides of the Atlantic.

Yours sincerely,

On behalf of the Article 29 Working Party,

Jacob Kohnstamm
Chairman

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013.

Website: http://ec.europa.eu/justice/policies/privacy/index_en.htm