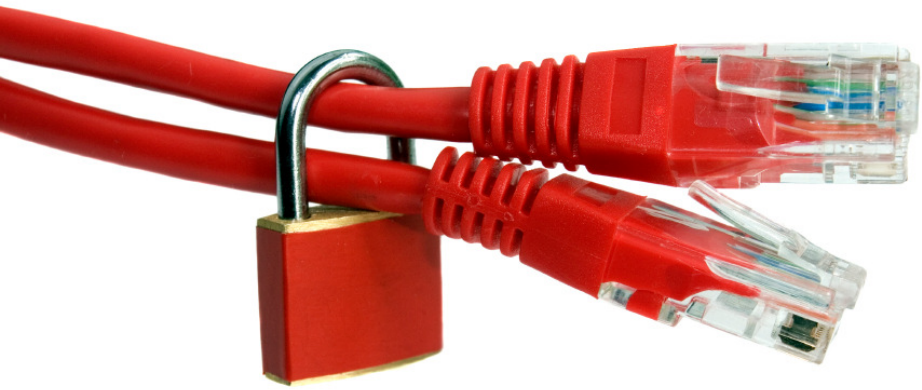


Implementing the EU 'cookies rule'

Guidance for National Implementation of the e-Privacy Directive

In association with:

EUROPEAN ASSOCIATION OF COMMUNICATIONS AGENCIES

EPC European Publishers Council

FEDERATION OF EUROPEAN DIRECT AND INTERACTIVE MARKETING

WORLD FEDERATION OF ADVERTISERS

Contents

This document has been produced as a guide to assist in the interpretation of the legal requirements but readers must not to take the opinions expressed as professional legal advice

For more information please contact:
Malte Lohan at WFA m.lohan@wfanet.org
Dominic Lyle at EACA dominic.lyle@eaca.be
Angela Mills Wade at the EPC angela.mills@wade.uk.net
Mathilde Fiquet at FEDMA mfiquet@fedma.org

Published December 2010

Executive Summary

In December 2009 the EU adopted the revised e-Privacy Directive, which amends among other things, the rules for obtaining users' consent when dropping cookies on their computers. Cookies are tiny files, composed of a string of letters and numbers, used by internet browsers to improve the operation of the web (storing passwords, measuring website visitors, helping sites load faster etc). Cookies are also the main technology used for improved targeting of online advertising.

The wording of the revised law, currently being transposed by Member States, is unclear, leaving considerable room for different interpretations at national level. In a worst case scenario, the new law could be interpreted as a requirement for "opt-in", i.e. requiring prior user consent each time the user is about to "receive" a cookie. This would significantly disrupt users' online experience and undermine marketers' ability to effectively engage consumers online.

The European advertising and media industry is therefore working closely with the European Commission to agree a suitable self-regulatory response. This will ensure

- enhanced transparency through easy to understand information about the use of cookies by advertisers and how advertising is based on consumers' interests

- consumer notification of data processing via a recognisable icon

- meaningful, easy to use consumer control over whether or not they want cookies to be used for the purposes of collecting data for advertising targeted to their interests

- independent consumer redress through trusted complaints handling procedures

In view of the transposition of this European directive into national law, advertising industry partners, including the media, will need to work closely together at national level to avoid overly restrictive transposition of the EU requirements and to shape national legislation that recognises self-regulation as fulfilling the EU consent requirement for cookies. This advocacy by the industry is essential in order to stave off the negative business impact on advertising and publishing of a mandatory opt-in requirement.

This guide is designed to facilitate this national outreach effort by providing common messages and arguments in favour of a proportionate implementation of the Directive for companies and associations.

Why this guide?

Directive 2002/58 ('the e-Privacy Directive') laid down the rules for the processing of personal data and the protection of privacy in the electronic communications sector. Its provisions applied to a number of digital advertising tools, including SMS, emails, automated calling machines, and targeted online advertising (***interest-based advertising – IBA***).

The 2002 e-Privacy Directive was reviewed in 2009 and the rules on the use of cookies were amended.

Why cookies are vital for the internet economy

Cookies are essential for making the web work. They allow websites to "recognise" users when they return to a site or browse from page to page and to "remember" their preferences: language settings, passwords, preferred content, shopping baskets etc. They also help websites better understand what users do on their pages and how they interact with ads, and so improve their functionality and content.

Importantly, cookies are one of the main tools used for interest-based advertising: helping to make sure that online advertising is better tailored to users' interests, and therefore more relevant and effective.

As this is a Directive (as opposed to a Regulation), Member States have some flexibility in implementing the new rules. Governments have until **25 May 2011** to implement the revised Directive (though in practice transposition deadlines are rarely met by all Member States).

The risks that online advertising is severely hampered during this process of national implementation are considerable. The new provisions are unclear and allow for potentially damaging and/or divergent interpretations. In a worst case scenario, the new law could be interpreted as a requirement for opt-in, i.e. prior consent every time certain types of cookies are used. This would require incessant pop-ups or prompts requesting consent, seriously disrupting users' online experience and fundamentally undermining marketers' ability to effectively engage consumers online.

In view of the ambiguity in the text of the Directive, it is essential that the European advertising and media industry implements a coordinated outreach effort, on the basis of a common strategy, to shape the implementation of the new rules at national level.

Through EASA (European Advertising Standards Alliance), the advertising and media industry, together with national advertising self-regulatory organisations are working in partnership with European Commissioner Neelie Kroes who is responsible for the Digital Agenda and Robert Madelin, Director General of DG Information Society. Although the Commission will not endorse formally our self-regulatory framework they are prepared to promote it to Member States Governments so long as we meet their minimum criteria, as set out by the Commissioner on 17th September 2010:[1]

1. "First and foremost, we need effective transparency. This means that users should be provided with clear notice about any targeting activity that is taking place.

[1] http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/452

2. Secondly, we need consent, i.e. an appropriate form of affirmation on the part of the user that he or she accepts to be subject to targeting.
3. Third, we need a user-friendly solution, possibly based on browser (or another application) settings. Obviously we want to avoid solutions which would have a negative impact on the user experience. On that basis it would be prudent to avoid options such as recurring pop-up windows. On the other hand, it will not be sufficient to bury the necessary information deep in a website's privacy policies. We need to find a middle way. On a related note, I would expect from you a clear condemnation of illegal practices which are unfortunately still taking place, such as 're-spawning' of standard HTTP cookies against the explicit wishes of users.
4. Fourth and finally: effective enforcement. It is essential that any self-regulation system includes clear and simple complaint handling, reliable third-party compliance auditing and effective sanctioning mechanisms. If there is no way to detect breaches and enforce sanctions against those who break the rules, then self-regulation will not only be a fiction, it will be a failure. Besides, a system of reliable third party compliance auditing should be in place."

In order to assist this process, this guidance document covers the following:

1. **Overview of online advertising and the privacy debate**
2. **The new e-Privacy Directive: how to interpret the consent requirement**
3. **The strategy of the European advertising industry**
4. **Guidance to national industry representatives**

Overview of online advertising and the privacy debate

Key message: Talk about *interest-based* advertising (avoid 'behavioural'); call it *consumer control* (not 'opt-out') and get familiar with cookies terminology.

The rapid growth of digital marketing communications, while offering tremendous opportunities for marketers, has raised consumer protection concerns, regarding data protection, consumer privacy and fairness of commercial practices among others.

Interest-Based Advertising (IBA) raises particular concerns because of its reliance on the collection and processing of consumer data, mainly through the use of cookies. Criticism centres on the lack of *transparency* and *user control* which marketers provide for this practice. The protection of children and the use of sensitive data for the purposes of advertising are also at the heart of the debate

Important technical and language specifications

As this is a highly controversial field, the choice and accurate use of terminology is important. Here are some guidelines:

Interest-based advertising: The online advertising techniques using cookies and similar tools to tailor advertising better to users' interests should be called interest-based advertising, or IBA. Typically, these interests are inferred on the basis of users' web viewing patterns over time and across websites (sites visited, links clicked, videos watched etc). Although this is sometimes also referred to as *Online Behavioural Advertising* (OBA), IBA is a more accurate way to describe this practice. Other expressions like *profiling* should be avoided, as they do not accurately reflect the nature of IBA but often carry negative connotations in a political context.

IBA uses anonymous data from cookies: it does not use any personal data like names, emails etc. It works by building "***interest segments***" linked to the browser on the basis of the users' web viewing patterns: for example sports, fashion, travel etc. Users are then served ads relevant to the interest segments that their browser is associated with.

It's important to distinguish IBA from ***contextual advertising*** which is not subject either to criticism or the self-regulatory framework. One of the ways to make the ads relevant is simply to use the context of the web page where the ad appears: the sports section of Time.com contains codes which inform ad networks that this is the sports section, and this may simply prompt an ad relevant to that context – for a sports equipment website, for example. Contextual advertising of this type raises no particular privacy questions.

Retargeting: A slightly different and increasingly popular form of IBA is called retargeting. Retargeting refers to ads that are delivered to consumers based on their browser's previous engagement with a specific product or service online that did not result in a specified action. For example, if a visitor of an online shop puts product A in his shopping cart but ultimately fails to make the purchase, he may later be retargeted with ads featuring the same product A on other,

unrelated sites. Retargeting allows companies to continue the marketing conversation with existing or prospective customers after they leave the company's website.

Opt-in/opt-out? *Consumer control!* Until now, the ways in which online users may give their consent to receive IBA have typically been described in a basic dichotomy of 'opt-in' versus 'opt-out'.

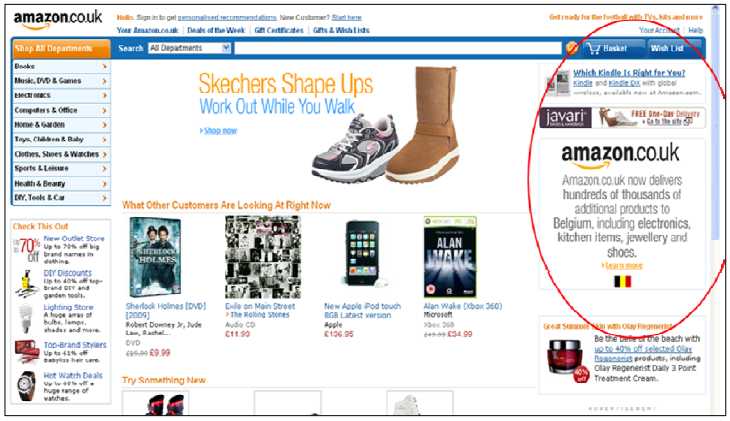
- **Opt-in** means that online users give their prior and express permission to receive IBA from that point in time onwards on the basis of their past web viewing behaviour.
- **Opt-out** means that online users are already receiving IBA and have the possibility to stop receiving (i.e. 'opt-out' of) such communications.

If the choice is between a stereotypical opt-in and opt-out approach, the former is usually seen by policy makers as offering stronger protection for consumers. By implication, when industry opposes an opt-in approach it is seen to be asking for 'less' consumer protection.

However, the opt-in/opt-out juxtaposition is a false dichotomy: digital tools can enable a more dynamic, real-time, form of consent which cannot be reduced to a simple opt-in or opt-out: it provides a high level of consumer control without constantly interrupting users' online experience. It is this type of dynamic consent on the basis of clear and comprehensive information that is at the heart of industry's self-regulatory initiative. We therefore recommend you describe the industry's preferred mode of consent as effective **consumer control based on enhanced consumer information** instead of opt-out.

Cookies: A cookie, also known as a **web cookie**, **browser cookie**, and **HTTP cookie**, is a piece of text stored by a user's web browser. It is not a programme, and it doesn't "do" anything to a computer. Cookies are central to the effective operation of most websites. They can be used for authentication, storing visitor preferences on a given site, shopping cart contents, or anything else that can be accomplished to improve the interaction between that website and the visitor through storing text data. IBA relies on different sorts of cookies, depending on who is responsible for dropping and retrieving/processing them later on. It is important to make a clear distinction between cookies and "spyware" or "malware" – types of malicious software used to secretly access a computer system without the owner's informed consent. This type software is illegal; cookies are perfectly legitimate.

- **First-party cookies** are set by the same website that a user is visiting. For instance, when users visit amazon.com, one or more cookies will be dropped and managed by Amazon directly. These cookies will inform Amazon about e.g. statistical data (length of



visit, number of clicks, browsing behaviour…) but also about interests and preferences for future visits. First-party cookies are what allow Amazon to recommend books to their users based on the items they've previously purchased, their location/language etc.

- **Third-party cookies** are placed on a user's computer by a third party - for example, a company that sells advertising on a website's behalf – and not that particular website owner. The cookies used for the purposes of IBA are primarily third-party cookies. Through contractual agreement with the website publisher, they are placed by ***ad networks*** when users visit one of their partner sites, and allow the ad network to identify that users' browser across their partner sites and to build interest segments linked to that browser.

Through their ***browser settings***, users can delete cookies stored on their computers manually or automatically (e.g. at the end of each session, every month). Users can also choose to authorise first-party cookies only, or they may refuse cookies altogether. Most browsers, such as Mozilla Firefox, Internet Explorer and Opera, allow third-party cookies by default.

Flash cookies (also known as Flash Local Shared Objects) are very similar to traditional cookies, but they are not placed and managed through the normal browser. Flash cookies operate with the Flash plug-in used to display all kinds of content (animation, Web apps, text and images). Instead of using the browser's local storage system, though, Flash cookies have their own. In other words, the Flash plug-in is able to store data locally just like a user's browser does, but in a different location on the hard drive. The implication is that built-in browser controls that enable the user to control standard cookies don't usually work with Flash cookies. As a result Flash cookies pose greater privacy concerns, and would be particularly controversial if used for IBA purposes.

Flash cookies have been making headlines recently because of reported cases of so-called "***re-spawning***" – where Flash cookies are used to re-instate standard HTTP cookies that have previously been deleted by a user. The industry strongly condemns this practice and our self-regulatory framework makes it clear that this is illegal.

The new e-Privacy Directive: how to interpret the consent requirement

Key message: The new consent requirement in the Directive is not by definition '*opt-in*', but rather enhanced **consumer control** on the basis of easy to find and clear information.

The key issue at stake is the clause amending the consent requirement for cookies (article 5(3)). It is important to note this does not apply to all types of cookies. "Technical" cookies used simply to enable a website to function properly (e.g. language settings or shopping cart functionality) are not subject to the consent requirement. The intention of the new rules is to obtain user consent for "non-technical" cookies, and third party cookies like those used for IBA in particular.

A transposition which would translate article 5(3) into a *prior* consent requirement (i.e. opt-in) must be avoided. An opt-in regime would require internet users expressly to request – by of means of e.g. pop up windows or similar prompts – a number of cookies dropped in any given session (they can easily reach several dozen). This form of consent would evidently be highly detrimental to users' online experience. Furthermore, as a majority of consumers could be expected to refuse to opt-in, this would undermine the ability of marketers to provide more relevant and effective advertising online.

It is therefore critical to note that the refined wording of the new ePrivacy Directive does not explicitly call for opt-in consent for cookies enabling IBA. This interpretation is supported by the following 4 key points:

a. The text of the Directive does not include the word "prior"

Article 5(3) of the ePrivacy Directive provides that:

"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" [Emphasis added].

So what's new? The new vs. old article 5(3):

Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned…

Old article 5.3	**New article 5.3**
..is provided with clear and comprehensive information *in accordance with Directive*	***…has given his or her consent, having been provided with clear and***

95/46/EC, inter alia about the purposes of the processing, ***and is offered the right to refuse such processing by the data controller.*** *(…)*	***comprehensive information****, in accordance with Directive 95/46/EC, inter alia about the purposes of the processing.*

The new wording indicates that some form of user consent is required to drop a cookie i.e. "storing information or gaining access to information already stored". The explicit requirement for "*prior consent*" does not appear in the text of the Directive. This is not a mere oversight, but a clear indication that the legislator's intent was not to insist on prior consent especially when read with the accompanying, relevant Recitals to the Directive which imply consent can be gained via browsers or other technical means (see b. below).

Importantly, not all language versions have the same exact wording. While the English version above does not specify the nature of the consent to be given, some language versions are more prescriptive:

English	French	German	Spanish	Italian	Dutch	Portuguese
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,	n'est permis qu'à condition que l'abonné ou l'utilisateur ait donné son accord, après avoir reçu, dans le respect de la directive 95/46/CE, une information claire et complète,	nur gestattet ist, wenn der betreffende Teilnehmer oder Nutzer auf der Grundlage von klaren und umfassenden Informationen, die er gemäß der Richtlinie 95/46/EG u. a. über die Zwecke der Verarbeitung erhält, seine Einwilligung gegeben hat.	a condición de que dicho abonado o usuario haya dado su consentimiento después de que se le haya facilitado información clara y completa,	sia consentito unicamente a condizione che l'abbonato o l'utente in questione abbia espresso preliminarmente il proprio consenso, dopo essere stato informato in modo chiaro e completo,	alleen is toegestaan op voorwaarde dat de betrokken abonnee of gebruiker toestemming heeft verleend, na te zijn voorzien van duidelijke en volledige informatie	só seja permitido se este tiver dado o seu consentimento prévio com base em informações claras e completas,

These diverging translations risk creating obstacles to the consistent implementation of the Directive throughout the 27 Member States. Although there is no single linguistically authoritative version, the English wording should be strongly supported.

b. A recital of the Directive confirms this interpretation

Recitals in EU legislation have no legal binding force, but they are useful to interpret the spirit of the articles of the law, including before the courts. Recital 66 of the e-Privacy Directive is a helpful clarification of the wording of article 5(3); it confirms that the article should not be interpreted as calling for opt-in consent:

> *"Third parties may wish to store information on the equipment of a user, or gain access to information already stored, for a number of purposes, ranging from the legitimate (such as certain types of cookies) to those involving unwarranted intrusion into the private sphere (such as spyware or viruses). It is therefore of paramount importance that users be provided with clear and comprehensive information when engaging in any activity which could result in such storage or gaining of access. The methods of providing information and offering the right to refuse should be as user-friendly as possible. Exceptions to the obligation to provide information and offer the right to refuse should be limited to those situations where the technical storage or access is strictly necessary for the legitimate purpose of enabling the use of a specific service explicitly requested by the subscriber or user. Where it is technically possible and effective, in accordance with the relevant provisions of Directive 95/46/EC, the user's consent to processing may be expressed by using the appropriate settings of a browser or other application. The enforcement of these requirements should be made more effective by way of enhanced powers granted to the relevant national authorities."* [Emphasis added]

Recitals 17, 24, and 25 provide further helpful clarification

c. A group of 13 Member States signed a supporting statement

In response to the lack of clarity in the amended text, 13 Members States adopted a joint Council Statement on 18 November 2009 to clarify their intentions as regards the implementation of article 5(3) of the e-Privacy Directive. It reads:

> *"Article 5(3) of Directive 2002/58/EC concerns the conditions under which information, including unwanted spy programmes or other types of malware may be placed on an individual's terminal equipment. It also applies to "cookies" and similar technologies, the use of which may in many instances be legitimate. The amended text of Article 5(3) clarifies that the existing consent requirement for the use of such technologies, applies regardless of whether they are delivered via electronic communications networks or other technical means … However, as indicated in recital 52(a) {66}, the amended Article 5(3) is not intended to alter the existing requirement that such consent be exercised as a* ***right to refuse*** *the use of cookies or similar technologies used for legitimate purposes.*[2] *"* [Emphasis added].

While this statement has no legal binding force, it makes two important points:

- There should be a clear differentiation between cookies used for legitimate purposes and illegal software e.g. spyware or malware.
- The existing consent requirements are adequate, and the new law does not depart from the "right to refuse" as a sufficient condition for collecting data via cookies for legitimate purposes such as advertising.

[2] Excerpt from Statement by **Austria, Belgium, Estonia, Finland, Germany, Ireland, Latvia, Malta, Poland, Romania, Slovakia, Spain and the UK** on the e-Privacy Directive, Brussels 18 November 2009.

d. The European Commission supports a user-friendly solution

In her speech of 17 September 2010 to the European digital advertising industry, Neelie Kroes, European Commissioner for the Digital Agenda (in charge of the e-Privacy Directive), addressed the implementation of article 5(3). She confirmed the fact that the new provisions do not call for a opt-in consent. She stressed that "*we need a user-friendly solution, possibly based on browser (or another application) settings. Obviously we want to avoid solutions which would have a negative impact on the user experience. On that basis it would be prudent to avoid options such as recurring pop-up windows.*"

She also gave her support to a self-regulatory solution and insisted that the solution "*must be a driver, and not an impediment, to the growth of the digital economy.*"

Conclusion: The new article 5(3) does not require opt-in consent for cookies. That being said, governments are free to interpret the article as a requirement for gaining prior consent for the use of cookies, and pressure for such a requirement is clearly growing.

The Article 29 Working Party's Opinion on Behavioural Advertising

The Article 29 Working Party (Article 29 WP) is the EU's independent advisory body on data protection and privacy, set up under Article 29 of the Data Protection Directive 95/46/EC. This well-respected expert group consists of the 27 national data protection authorities and is considered to be an authoritative voice on data protection matters.

In an opinion published in June 2010, the Article 29 WP aimed to clarify "*how EU rules apply to online behavioural advertising*", including the revised ePrivacy Directive. It concluded by calling for prior opt-in consent to behavioural advertising – putting it at odds with the European Commission, a number of governments and the industry.

According to the opinion, Article 5(3) of the ePrivacy Directive and its Recital 66, along with the 1995 General Data Protection Directive, require prior opt-in consent since "*prior opt-in consent mechanisms are better suited to deliver informed consent.*"

According to the Working Party, browsers fail to deliver valid consent unless they reject third-party cookies by default, and convey clear, comprehensive and fully visible information. Ad network providers are thus encouraged to create prior consent mechanisms, which require the users to accept in advance the storage of cookies and the use of cookie data to track browsing across websites in order to deliver targeted advertising. The Opinion also states that consent must expire after a certain period of time, and that there must be a simple way for users to be able to revoke consent.

Despite this dissenting reasoning, the opinion nevertheless *"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."* While the Opinion has no legal force, it is likely to be a reference point during national discussions on implementing the e-Privacy Directive.

The strategy of the European advertising industry

Key message: In response to a clear call by the European Commissioner for the Digital Agenda, the advertising industry has prepared a self-regulatory response that complies with the requirements of the e-Privacy Directive. It lays down requirements for enhanced notice to consumers through clear language and the use of an icon together with effective and enforceable consumer control. National governments, when updating laws transposing the e-Privacy Directive, should recognise and reflect this agreement and be asked to avoid inflexible language requiring prior consent.

The European Commission is responsible for overseeing implementation of the e-Privacy Directive, and advising governments where the text of the Directive is not sufficiently clear. It will therefore play an important role in our effort to prevent European governments from adopting an opt-in consent requirement.

Neelie Kroes, European Commissioner for Digital Agenda, has set out her clear support for a self-regulatory solution to implement the new consent requirements of article 5(3) of the e-Privacy Directive. Her overall goal is to find "*a balanced and realistic solution*". However, she has also made it clear that the new consent requirement for cookies is not satisfied by the status quo (ability to opt out from cookies through browser settings). A new "middle ground" between a full opt-in requirement and a basic opt-out approach therefore has to be found.

The Commissioner has set the following core conditions for a successful self-regulatory solution for that would meet this objective:

- **Transparency:** users should be provided with clear notice about any targeting activity that is taking place.
- **Consent:** an appropriate form of affirmation on the part of the user that he or she accepts to be subject to targeting.
- **A user-friendly solution:** Possibly based on browser settings or similar, avoiding any solution which would have a negative impact on the user experience.
- **Effective enforcement:** A self-regulation system should include clear and simple complaint handling, reliable third-party compliance auditing and effective sanctioning mechanisms.

Failing to provide an SR system that satisfies these requirements by the transposition deadline (May 2011) would force the European Commission to push for regulatory solutions.

The EU advertising industry is therefore in the process of designing an EU-wide self-regulatory solution that fulfils the Commission's requirements, based on the model of the ambitious self-regulatory programme for IBA launched in the USA in 2009. While IBA is not synonymous with cookies, it is clear that politically, the profiling of data collected from cookies for the purpose of targeting advertising is the single biggest issue related to cookies. Delivering an effective self-regulatory solution for IBA should therefore significantly reduce the pressure for opt-in consent for cookies more generally.

The core component of the self-regulatory solution is a simple, standard icon appearing in all interest-based ads that will inform users that IBA is taking place, and give them an easy and effective mechanism for exercising control over IBA if they so wish.

Key elements of this self-regulatory framework:

- ***Scope***. It applies to '3rd party' IBA, i.e. ads targeted on the basis of user data collected across different websites and over time (third-party cookies).
- ***Notice***. A simple, standard icon appearing in interest-based ads to inform consumers that IBA is taking place, and provide access to detailed information about how and what data is collected if desired. If this user notice is not included in the ad itself, the code requires website operators (the 1st party) to inform users when data is collected for IBA.
- ***Choice***. Whichever the form of notice, 3rd party IBA providers must via this notice offer users the ability to control the use of data for IBA purposes. Companies which use data for IBA at 'service provider' level (e.g. at the level of the Internet access provider or the browser, which can essentially monitor all websites visited by a user) must ask users to opt-in.
- ***Children***. Industry will not create IBA segments which are specifically designed to target children under 13.
- ***Sensitive data***. In line with the law, IBA segments will not be created in sensitive areas (such as health, religion, political affiliation, etc.).
- ***Consumer Redress.*** Via independent, national advertising self-regulatory organisations, consumers will be able to complain or seek guidance about the consumer controls over their cookie and IBA choices.
- ***Monitoring of third party ad-networks.*** Providers of interest-based advertising which sign the framework will be subjected to independent monitoring to ensure technical standards of compliance are being met.

This framework will be hard-wired into the network of existing self-regulatory systems, and will therefore comply with the EU-Commission's endorsement of our best-practice model for self-regulation represented by the European Advertising Standards Alliance (EASA). This means that ***the Framework will become operational across the EU and will be enforced via familiar independent national complaint mechanisms.***

This initiative is designed to meet the EU's requirement for a self-regulatory solution that offers internet users transparency, control through a user-friendly consent mechanism, and effective enforcement. The European advertising industry is working with the European Commission to ensure that this self-regulatory solution is recommended in the guidance that the Commission is preparing for Member States to implement the ePrivacy Directive.

For this guidance to be followed by Member States, it is essential that the industry implements the self-regulatory initiative effectively and advocates it forcefully vis-à-vis national authorities.

Examples of IBA consumer notice in ad

Guidance to national industry representatives

While Member States work on transposing the new e-Privacy Directive in time for the May 2011 deadline, it will be essential for local industry representatives to engage actively to ensure that new rules do not hamper the opportunities for effective online advertising; and in particular that inflexible rules do not curb interest-based advertising. Instead please promote the self-regulatory alternative which provides for user-friendly solutions for consumer information and control. This advocacy effort should be based on the following key elements:

- **Promote the self-regulatory approach**: The revised e-Privacy Directive is ambiguous and leaves the door open to interpretations that would damage the industry and internet user experience, without increasing consumer protection. The industry has developed an effective self-regulatory solution in line with the intent of the Directive, which is to empower consumers to exercise informed choices about IBA. The EU will support this solution if industry can prove that it is user-friendly and effectively enforced. It is crucial for the industry to demonstrate its commitment to this self-regulatory solution and obtain government support for self-regulation at national level so as to avoid crippling regulation.

- **Cooperate with industry partners**: The provisions of the new Directive impact all players in the advertising industry: advertisers, online publishers, ad networks, agencies and self-regulatory organizations. Cross-industry buy-in to an effective self-regulatory framework and close cooperation for its implementation and national advocacy efforts is essential.

- **Re-focus the debate:** Data protection and privacy are politically sensitive and emotional subjects. Terminology such as "online behavioural advertising", "profiling", and "opt-in" vs. "opt-out" do not help our case. Focus on demystifying the subject and offering constructive solutions. Positive terminology:

    - **Interest-based advertising** – not online "behavioural advertising" or "online profiling"
    - **Consumer control** – not "opt-in" or "opt-out".
    - **Informed consent and transparency** – not "prior consent" or "explicit consent".

- **Key messages to national authorities:**

    - **The new e-Privacy Directive does not prescribe opt-in consent for cookies:** This would negatively affect users' online experience, undermine the potential of IBA and the growth of the EU's digital economy, and would not improve consumer protection.
    - **The new e-Privacy Directive calls for a user-friendly consumer control**: This vision is supported by many Member States and the European Commission. Coherent, proportionate interpretation of European legislation is particularly important in the context of the internet, which knows no frontiers.
    - **The advertising industry is implementing a self-regulatory framework across the EU that will provide user-friendly consumer control**: The framework will inform users about IBA and provide a simple tool to exercise their choices. Industry will put in place the necessary structures for effective enforcement. To enable this system to thrive, national laws should not undermine it and national authorities will need to support it.