Digital Window EU Privacy Directive Update: May 2011

Prepared by Kevin Edwards, Strategy Director

From 26 May, new European laws will come into force that dictate how web users can be tracked online. The changes will require technology companies, retailers and other suppliers that track information online (usually via cookies) to seek 'informed consent' from web users in order to do so.

There remains much confusion within the online community with what this means and what companies should be doing to ensure the services they offer to both consumers and clients are not adversely affected.

This document seeks to shed light on the current situation as well as highlight the key areas of debate.

It is worth noting that this document outlines the situation as it is at present. What is clear from government advice is there is much work and additional consultation ahead. This will hopefully provide clarity for individual businesses on what their approaches should be.

It is also clear a pan-industry approach provides the best opportunity for the most workable and obvious solutions. This document will outline what this could look like.

One of the worst outcomes would be for individual companies to develop their own solutions in isolation. This would undoubtedly lead to confusion, loss of transparency and potentially heavy handed enforcement.

In writing this document we have sought guidance from the Internet Advertising Bureau (IAB) who has been involved in the whole processes of helping to inform and provide practical solutions to ensure the new laws can be transposed into UK law with minimum disruption to the digital sector.

We have also heavily referenced the Government's advice published in April and May 2011 and the guidance of the Information Commissioner's Office (ICO) which is tasked with upholding individuals' privacy rights.

The e-Privacy Directive

Directive **2002/58** on Privacy and Electronic Communications, otherwise known as the **e-Privacy Directive**, is an EU directive dealing with data protection and privacy in the digital age.

In 2009, a revised e-Privacy Directive was announced that would be translated into law for each of the EU's member states. The revised Directive is part of a broader piece of European legislation – the EU Electronic Communications Framework - that comprises a total of five Directives and is required to be implemented into national laws by 26th May 2011.

The revised Directive will amend the existing one with a requirement now to obtain consent for "the storing of information or the gaining of access to information stored in the terminal equipment of a subscriber or user... having been provided with clear and comprehensive information" (Article 5.3).

It is also worth noting that the Directive deals with issues of privacy. Some commentators have assumed that alternative tracking solutions (such as first party cookies rather than third party cookies) would subvert the amendments to the Directive.

This misses the point; the work that needs to be done around privacy is the important element and all parties need to work collaboratively to demonstrate they are offering consumers and website users clarity and transparency when using the Internet, enabling them to make an informed choice about what information is stored.

This should be the overriding sentiment for all considerations.

Informed Consent

Much of the confusion surrounding the revisions to the Directive involves the notion of 'consent'. When the Directive's amendments were first drawn up, the language used indicated web users would be required to explicitly opt in to cookies when browsing the web.

This language has subsequently changed to concepts of 'informed consent', that is providing sufficient information to consumers about how their data is captured, in order for the consumer to make an informed choice about whether they give permission to do so.

'Informed consent' is now the standard we are working towards, NOT 'prior consent'. According to the latest Government advice published on May 24th 2011,

> *"'Consent' is defined in the Data Protection Directive as "any freely given specific and informed indication of his wishes"... Article 5 of the revised e-Privacy Directive does not specify that the consent must be "prior consent". **The original text proposed by the European Parliament did do so but this was removed during negotiation**.*
>
> *"Crucially, there is no indication in the definition as to when that consent may be given, and so it is possible that consent may be given after or during processing. It is important that stakeholders are aware that in its natural usage 'consent' rarely refers to a permission given after the action for which consent is being sought has been taken.*
>
> *"This absolutely does not preclude a regulatory approach that recognises that in certain circumstances it is impracticable to obtain consent prior to processing.*
>
> *"Crucially, the requirement of the revised Directive is for informed consent. It is this requirement that has shaped the UK approach set out above. **It is therefore the firm view of Government that the definition of consent employed in the amending regulation enables rather than precludes the O(nline) B(ehavioural) A(dvertising) Framework developed by industry**."*

This guide can therefore be interpreted that informed consent should be the facilitation of information for consumers about what data is being captured on site. The Online Behavioural Advertising framework as outlined here offers full disclosure of how data is used to target ads according to user behaviour. It also offers an opportunity to opt-out of receiving such advertising.

It is essentially an "information provision then opt-out if requested" solution. The information is also made available to users via a logo within banner creative. It requires a user to actively click on the logo and opt out.

The latest Government statement on OBA makes it very clear that the efforts by industry to address concerns about this most tangible use of cookies addresses key concerns:

> *"The UK approach has also been built around support for the cross-industry work on third party cookies in behavioural advertising. This the UK has championed in Europe and also in the Government response.*
>
> *"We believe that this work fully addresses one of the uses of cookies of most concern to users. It is, therefore, a major component in the Government's plans for meeting the requirement of the revised provisions."*

The OBA is one solution for one type of advertising. It is worth remembering that advertisers, networks and affiliates will be making use of a whole range of cookies and they will need to ensure they are aware of how these cookies operate and what information they capture.

As a general guide the ICO has stated:

> *"The more privacy intrusive your activity, the more you will need to do to get meaningful consent."*

We should all therefore be fully aware of the range of affiliate (and non-affiliate) cookies being dropped and how intrusive they are to the user experience. It's worth noting that if cookies are deemed strictly necessary to a service, e.g. remembering what is in a consumer's basket in order for them to transact online, then they are exempt from the revised Directive.

The ICO maintains the remit of 'strictly necessary' is narrow and only refers to those services that would make online activity difficult and to the detriment of the consumer:

> *"This exception needs to be interpreted quite narrowly because the use of the phrase "strictly necessary" means its application has to be limited to a small range of activities and because your use of the cookie must be related to the service requested by the user.*
>
> *"Indeed, the relevant recital in the Directive on which these Regulations are based refers to services "explicitly requested" by the user. As a result our interpretation of this exception therefore has to bear in mind the narrowing effect of the word "explicitly".*
>
> *"The exception would not apply, for example, just because you have decided that your website is more attractive if you remember users' preferences or if you decide to use a cookie to collect statistical information about the use of your website."*

It is unclear whether the use of cookies for cashback, loyalty and reward sites could be deemed strictly necessary although a strong argument could be formed to suggest they are.

Solutions

Technical solutions: Browsers

Article 5(3) of the e-Privacy Directive states that users' consent may be expressed by using the appropriate settings of a browser or other application. There has also been much discussion about using *existing* browser settings. The Government and ICO have stated categorically this will not be enough to satisfy the new Directive.

At the moment the ICO is also advising that browser settings in the near future should not be considered a viable platform for obtaining informed consent. That said, the UK Government stated in April that it is actively working with browser companies to explore possible solutions:

> *"The Government proposes to work with browser manufacturers to see if these can be enhanced to meet the requirements of the revised Directive - users will be provided with more information as to the use of cookies and will be presented with easily understandable choices with regard to the import of cookies on to their machine.*
>
> *"In terms of taking this work forward, Government has formed a working group made up of representatives from the browser manufacturers to look at the issue in more detail."*

In the latest Government response published on 24th May this was reiterated:

> *"(The Government) set out proposals to continue to work with browser manufacturers to see if browsers can be enhanced to meet the requirements of the revised Directive... the development of enhanced browsers that meet the information requirements of the revised Directive are being pursued in collaboration with industry."*

It is clear that browser settings offer the easiest and most consensual approach to addressing some of the Directive's major concerns.

This is clearly a work in progress and we watch the developments with interest to see how this develops over the coming year.

Technical Solutions: Pop-ups

Pop-ups requiring users to agree to sharing information are considered a potential option. The ICO has referenced this as a possible technical solution but without a precedent it is unclear what this could look like, what message would need to be communicated and whether a one off opt-in/out would be sufficient. Technical solutions would also need to be developed enabling consumers and users to opt-out of cookies.

What you should do

Affiliate marketing has always been one of the most forward thinking digital channels. The Affiliate Marketing Council's (AMC) enlightened approach has created an effective self-regulatory framework that has successfully launched key best practice initiatives since 2009.

In 2011, a sub-committee aimed at addressing pending digital legislation was formed. This is now the central conduit for information about the e-Privacy Directive.

You can find out more about the AMC here: www.iabaffiliatemarketing.com.

The site will feature regular updates about the e-Privacy Directive together with the latest ICO and UK Government advice.

The ICO advises websites to take the following steps:

1. Check what ***type of cookies*** or similar technologies you use and how you use them
2. Assess how ***intrusive*** your use of cookies is
3. Decide what solution to ***obtain consent*** will be best in your circumstances

The ICO hasn't provided a prescriptive list of actions and what to do in order to address the above, but it is worth (as part of your due diligence) being aware of at least the first two points and compiling a document outlining your findings.

It is also clear the following two initiatives will prove crucial in deciding what we all need to do about point three:

1. The OBA self-regulatory framework
2. Browser solutions

Both of these points have been addressed in this document.

Additional work that could be considered by the affiliate industry is a similar initiative to the OBA framework, although that is likely to be an information exercise rather than an 'opt-out' technical solution in the short term.

Longer term, a technical committee could be formed to provide possible opt out solutions for consumers and users on sites making use of affiliate links. This discussion is in its embryonic stages. Again the AMC blog is the best place to keep up to date on any developments.

Ultimately the UK Government has instructed the ICO not to enforce anything for at least twelve months from 26th May 2011:

> *"The Government response made clear that enforcement action will not be taken until appropriate technical solution are available."*

On 25th May the communications minister, Ed Vaizey told web businesses that "there will be no immediate changes to how UK websites operate as a result of new EU rules". Instead, he says he will work with the digital industry to "come up with workable technical solutions" before any enforcement.

He added the Government was committed to a ***"light touch, business friendly"*** approach to cookies that ***"sets a benchmark for Europe".***

In conclusion the message is clear, don't panic, hold tight and keep up to date with wider industry initiatives. However, as part of a due diligence exercise, it is definitely worth familiarising yourself with cookies and how your site uses them.

Further reading:

UK Government Open Letter, 24th May 2011
ICO Advice, 9th May 2011
UK Government Consultation Document, April 2011
The AMC Blog
IAB Europe Online Behavioural Advertising Framework, April 2011
The IAB (UK)