Cookies and European Law 2012

### Introduction

In 2009 the European Commission issued an amendment to the 2003 E-Privacy Directive requiring consent for the storage of information on user devices. The British Government, and all other member states, passed this into law in 2011. Prior to this the government made it clear that there would be lead in phase of 1 year allowing businesses time to prepare for the changes. This so called “amnesty period” comes to an end in May 2012.

In their latest guidance document, the British government’s information regulatory office, the [Information Commissioner’s Office](http://en.wikipedia.org/wiki/Information_Commissioner%27s_Office) (ICO), offers detailed guidelines on how businesses might comply with the new regulation.

There follows a brief outline of the December 2011 guidelines.

### Why now?

The legislation was prompted by concerns about online tracking and spyware i.e. information stored on users PC’s which is used to identify them without their knowledge.

### What does it cover?

It covers cookies (to both persistent and non-persistent), “Shared objects” (e.g. Flash Cookies and Silverlight Isolated Storage objects) and web bugs (e.g. information hidden in gif files).

Importantly it applies to any information about a user and **not** just PII.

### Consent

There are three classifications of consent. Understanding these is important in assessing any necessary compliance measures.

#### Prior

This describes the act of getting consent after a cookie has already been created. This is not how consent normally works and is likely to confuse users. In the case of older web sites the ICO suggests that this will be acceptable provided there is a prominently displayed “About Cookies” in the sites header area, and site owners show that they’ve made some effort to reduce the intrusiveness and life time of such cookies.1

#### Implied

Where it is assumed the user knows that cookies are being used. In the future when browsers allow users to configure their preferences this will constitute “implied consent”. However browser based opt-in strategies are not widely supported at present. In fact the success of these future opt-in strategies is, in part, dependent upon the current generation of web sites educating users about cookies.

Making users aware, with very prominent links to information about such cookies, is the advised approach to maintaining compliance.2

### User/Subscriber Services

This describes issues around services a user or subscriber3 has signed up for and which requires cookies to work correctly.

Making information about cookies clearly visible, along with option’s to disable them for existing web sites will suffice.4 For new build web sites, consent will need to be gained prior to setting any cookies. This might take the form of a check box clearly labelled on the T’s & C’s screen for example.

Incidentally, no distinction is made between the user/subscriber parties as far as consent goes. It is an interesting distinction though, and is intended to distinguish a business user acting on behalf of a business, and home user acting on behalf of themselves.

### Cookie Types

There are a few different categories of cookie. Each has its own particular challenges, which we’ll now look at.

#### Session Cookies

These are used to overcome the stateless nature of the HTTP protocol in tracking a user’s interactions with a web site during each visit. They exist only as long as a user is viewing a web site and are removed when the browser hosting the session is closed. For this reason they are viewed as less intrusive and if used simply to support the sites functionality are deemed to be exempt from a requirement to gain consent.5

#### Persistent Cookies

These are cookies persisted between sessions. They can be shared across several sites and can be used to target advertising, or to record visitors preferences, or for analytical purposes. These types of cookies do require consent.

#### First and Third Party Cookies

First party cookies are those placed by the “originating domain” while third party cookies are placed by a domain not being visited by the user. If a site is placing third party cookies on behalf of a third party, the ICO recommend that the site owners have a contractual agreement with this third party governing their cookies behaviour.6

### What to Do

Doing nothing is not an option and is likely to bring the site owner into conflict with the law.7

The ICO recommends taking the following steps:

1. Perform an audit of cookies being used i.e. identify cookies and their purpose, the data they hold, any links to PII data, their life time, their originating domain, and check existing privacy policy
2. Assess how intrusive they are
3. Where consent is deemed necessary decide how it might be obtained

The IOC guidance document then goes on to advise on a number of practical ways to acquire consent. These are mostly common sense but the more interesting are:

* In the case of Services being offered consent could be part of the T’s and C’s
* If the site has a user setup it could be obtained as a step in the setup process
* If the site offers features that require 3rd party cookies enabling such feature might require consenting to cookies

### Further Reading

See the ICO guidelines [here](http://www.ico.gov.uk/~/media/documents/library/Privacy_and_electronic/Practical_application/advice_on_the_new_cookies_regulations.ashx).

For information about cookies in general the “All About Cookies” web site is hard to beat. It is located [here](http://www.allaboutcookies.org/).

1 IOC Guidance on the rules on use of cookies and similar technologies [December 2011] p. 6

2 as above p. 6-7

3  A subscriber is in the party which pays for the line (important in the case of a business) and a user is, well, a user.

4 as above p. 7

5 as above p. 8-10

6 as above p. 10

7 A fine of up to £500 000 is the maximum penalty the ICO can impose.