



Don't fall foul of the Cookie Monster

Website providers must now obtain explicit consent from visitors to their website before implanting cookies on visitors' computers or mobile devices.

Created using computer code rather than chocolate chips, cookies are text files that are implanted on the hard disks of website visitors. They collect information about website visitors such as their names, addresses and user preferences.

Cookies enable online providers to build profiles of users, their online behaviour and their interests. This data may be sold to third parties for a fee. Website providers who do not collate personal information themselves may even sell space on the website to third parties (usually advertising agencies) who collate this information instead.

The use of cookies undoubtedly raises concerns over users' rights to privacy, but cookies are in fact valuable components in the way we browse the web. For example, websites use cookies to 'remember' what is placed in your shopping basket whilst you browse other pages on the website. Without cookies, online shopping would be much more difficult. Some websites, such as Amazon, will use cookies to populate the homepage with items of interest to you based on past purchases and browsing patterns.

However, in an environment where privacy (and rather maintaining privacy) commands such a high value, the new laws were surely inevitable?

Website providers must now obtain a user's informed consent before implanting cookies. Such consent must also be actively given. It will not be sufficient for a website provider arguing that consent was implied by the website user since they did not alter their browser settings to reject cookies.

There are exceptions to the consent rule, but these exceptions are to be interpreted quite narrowly. Consent need not be required, for example, to a cookie used to remember what products a user chose to add to their shopping basket on a previous page. Also, if a cookie is "strictly necessary" for providing the service requested by the user, consent is not required.

Since the exceptions are so limited, specialist legal advice should be sought and if in doubt, consent should be obtained.

The Information Commissioner's Office has suggested that website providers obtain a user's consent by introducing pop-ups and similar techniques. This may, however, spoil the user's experience, not to mention impractical if a pop-up blocker is employed.

An alternative way to comply might be to revise the terms and conditions which users will have to consent to by clicking a box when signing up or registering with a website.

Problems arise for website providers who allow third parties to set cookies on their website. It would be logistically difficult in practice for website providers to ensure that the user is made aware of how the information of third parties will be used.

The issue of consent, and how to obtain it, is an area of concern for businesses and whilst the new requirements are flexible they are onerous and uncertain. The government has said that there should be a phased approach to the implementation of the new rules; compliance must be achieved by May 2012. Failure to comply after this time could result in a fine from the ICO of up to £500,000, albeit for severe breaches. Further guidance on how the ICO will enforce the new rules is expected later this year.

Nonetheless, the rules cannot be ignored and businesses should plan ahead and take action now by checking what type of cookies and other similar technologies they use, how often they use them and assess how intrusive their use of cookies is by deciding what solution to obtain consent will be best in their circumstances.

If you have any queries about the new rules relating to cookies or any other company or commercial law related issues please contact the Smith Partnership Company Commercial Team on 01332 225225.



**Elizabeth Mills,
Company Commercial
Solicitor**

