

## **Taking more than the biscuit?**

---

Today "cookies" are an essential function of many websites seeking to sell products and services to their users. Since their "birth", however, cookies have created privacy issues due to their ability to track user behaviour - and by tracking we mean they know "what you did last night", at least on the web anyway!

With the implementation of the Privacy and Electronic Communications Directive 2002/58/EC (the "Directive"), website operators were finally forced to sit up and take account of our privacy concerns, ensuring that when we use their websites they must tell us in a "clear and comprehensive" manner the "purposes of the storage of, or access to, that information", and ultimately, websites must provide us with the opportunity to refuse such storage of, and/or access to, that information.

We have however moved onto the next generation of cookies, the "Flash cookie" (albeit they have in fact been around now for several years). The newer Flash cookie can potentially store much more information about your browsing activities, but more importantly you can't find them on your web browser, resurrecting the old problem of "does the user know they are there, and how can they get rid?"

### **Getting Flash**

An academic study by researchers at the University of California in Berkeley ([http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1446862](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862)) has found that over half of the top 100 websites are retaining user information about us through Flash cookies without permission. This will be of particular concern to those who try to delete cookies as a means of keeping their internet browsing patterns private. Flash cookies differ from HTTP cookies (which users can delete on request), in that they remain largely undetected by privacy settings on your web browser such as Internet Explorer or Firefox.

Flash cookies, many of which are capable of tracking user activity, originate from coding contained in Adobe's Flash media player. The player is usually made available to you for free and is often required so that you can run animations, movies, adverts etc on the website you are visiting. In several cases where researchers attempted to delete or block HTTP cookies on Flash-enabled sites, the Flash cookies continued to trace user data and even "re-spawned" the deleted information the next time they visited that same site. Only four of the 100 sites mentioned the use of the Flash technology for tracking purposes in their privacy policy. It is therefore likely that many individuals will be having their privacy breached without their knowledge every time they visit a web page.

### **Change of onus**

Under the terms of the directive, each "user", a data subject, must be provided with sufficient information about what the cookies are used for (traffic analysis and advertising, for example) to enable them to come to an informed decision and either provide or not provide their "consent", as set out in the Privacy Directive 95/46/EC and requisite domestic legislation, to the processing of their data.

This right (there is an exception for cookies necessary for the provision of a service expressly requested by a user) is generally provided by way of an opt-out under which the web provider will (or should in theory) no longer deliver, for example, advertisements which have been tailored to your web preferences and usage patterns. How the user is/was provided with this information and opt-out has until now been left open to interpretation, and website operators across Europe have tended to put in place an "easy to find" privacy policy, within which the relevant information has been placed.

The EU, however, has brought in a new set of reforms to the Directive\* which aim to provide, *inter alia*, greater regulation of "behavioural advertising", and must be implemented by member states within 18 months. In relation to cookies, the new law states that a user must explicitly choose to opt in to any website which intends to utilise behavioural tracking techniques. This is essentially a quite remarkable move away from how website operators deal with matters currently, where users must expressly opt out of having their browsing habits tracked.

Once the EU's reforms package has been adopted by member states, it will be no longer be sufficient for websites to rely on a user's browser security settings as a means of evidencing a user's consent to the use of all cookies on a particular website (HTTP cookies can usually be administered through a web browser's preference drop-down); explicit consent must be sought before applying their cookies on each webpage. Whilst it may not be "commercially convenient" to ask users' permission before serving each cookie, it is the most privacy-sensitive approach to the problem. A headache nonetheless, and yet another compliance issue for website providers across the EU.

To get rid of flash cookies and stop more appearing, instructions are available at <http://epic.org/privacy/cookies/flash.html>.

\* EU Telecoms reform package amending Directives 2002/22/EC (Universal Service Directive) and 2002/58/EC (Directive on privacy and electronic communications).

**Valerie Surgenor is a Senior Associate in MacRoberts. For more information please contact [valerie.surgenor@macroberts.com](mailto:valerie.surgenor@macroberts.com)**

**This article appeared in the February 2010 issue of The Journal.**

[See our website for full Copyright notice and Disclaimer.](#)

© MacRoberts LLP 2010