

ALERTS AND UPDATES

European Union Confirms "Get-tough" Approach on Cookies

August 31, 2011

The European Union's (EU) Article 29 Working Party confirmed in [documents](#) released this week its "get-tough" attitude on cookies ahead of a scheduled meeting with the advertising industry to discuss Europe's new cookie transparency laws next month. The Article 29 Working Party also confirmed that it was in discussions with the U.S. Federal Trade Commission to try to agree on a joint EU/U.S. approach to online behavioral advertising.

The Article 29 Working Party was set up as an independent European advisory body on data protection and privacy. It is run from Brussels, but the Working Party has representation from each of the 27 EU member states.

The debate on cookies has persisted for some time in Europe. In our [23 May 2011 Alert](#), we looked at the background to the new cookie laws in Europe, which should have become law in each EU country on 26 May 2011. Implementation has so far been mixed. Some EU countries met the deadline, but others did not. The UK met the deadline for introducing new legislation, but the UK's privacy regulator, the Information Commissioner's Office (ICO), has said that it currently intends to have a period of grace until next May, during which time prosecutions are unlikely. The new laws affect all cookies on any website, although online advertising has been the focus of much of the activity thus far.

The main issue with online advertising is the need to obtain consent before putting a cookie on a user's machine. Cookies power Internet advertising and are used to make sure that the right advertisement is served to the right user, to ensure the effectiveness of advertising campaigns and to provide usage information to make sure those hosting the ads get paid. Under EU rules, consent has to be "freely given, specific and informed. It must also be an indication of the data subject's wishes." The Article 29 Working Party says, "In practice, in the context of online behavioral advertising, this means that to obtain consent, ad network providers must provide the necessary information before the cookie is sent and rely on users' actions (e.g., clicking a box stating "I accept") to signify their agreement to receive the cookie and to be tracked for the purposes of serving behavioral ads."

In practice, this is likely to be unworkable for many in the world of the Internet. This may especially be the case when the Article 29 Working Party appears to cast uncertainty on the use of browser settings to imply consent. The Article 29 Working Party says that users cannot be said to have consented simply because they use an Internet browser that by default allows cookies.

September's meeting was arranged with the industry for industry representatives to update the Article 29 Working Party on their proposals for an icon scheme to be used to imply consent. The idea is that an icon would appear next to an online ad in much the same way as a padlock was used to indicate a secure site. The user would be able to click on the icon to get more information on the ad, the data being collected and where it was going. The Article 29 Working Party has a number of issues with the proposed scheme that are to be discussed with the industry next month.

In the short term, the position remains rather uncertain. Enforcement of the cookie laws is down to individual EU countries, not the Article 29 Working Party or the European Commission. As a result, enforcement is likely to vary across Europe. Businesses may want to consider acting promptly to ensure they know exactly the types of cookies their site is using. This would include auditing the practices of third parties who supply services to their website, such as order tracking; payment

fulfilment; or investor-relations content. The ICO has suggested a specimen cookie disclosure table, which businesses might want to consider in addition to full disclosure in their privacy policy. Even that might not be enough. As we reported in our *May Alert*, businesses should work on ways of telling visitors to their sites what is happening with their data. Given that the law is in a state of uncertainty, transparency should be the guiding principle of any business in its online activities.

For Further Information

If you have any questions on this *Alert*, please contact [Jonathan P. Armstrong](#) in our [London office](#), any of the [members](#) of the [Information Technologies and Telecom Practice Group](#) or the attorney in the firm with whom you are regularly in contact.

Disclaimer: This Alert has been prepared and published for informational purposes only and is not offered, or should be construed, as legal advice. For more information, please see the firm's [full disclaimer](#).