

Alerts and Updates

UNITED KINGDOM ACTS TO REGULATE COOKIES

April 20, 2011

The United Kingdom government announced on 15 April 2011, its long-awaited response to its consultation on new laws for Web cookies and e-commerce. Duane Morris participated in the consultation process. The main body of the [government's response](#) is 75 pages long with further appendices attached. The consultation was triggered by a new European Union directive (the [E-Privacy Directive \(2009/136/EC\)](#) or the "Directive") introduced at the end of 2009. That new Directive means that each of the 27 EU member states need to update their laws to deal with issues like cookies and security breach reporting by 25 May 2011.

Cookies

In introducing the new law, Ed Vaizey, the Minister for Culture, Communications and Creative Industries, called the new cookies consent requirement one of the most significant changes that website operators must undertake to implement the Directive. Cookies are important to the online world as they power advertising, which in turn makes the free-to-air model of most websites viable. The government's response recognizes that cookies are now a part of Internet life, saying "the Internet as it is today would be unusable or severely restricted without their use." Vaizey said that legislation to adopt the new cookie rules will shortly be introduced to Parliament to comply with the 25 May deadline.

The government's preferred approach is to work with browser manufacturers on a solution that will use enhanced browser settings to obtain the requisite "opt in" consent. It will also support cross-industry work on third-party cookies in behavioral advertising. This is something that the author (and Duane Morris) argued for in representations and an approach which also mirrors some industry initiatives in the United States. The government says "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 [onto] their machine."

Security Breach Notification

In addition to cookies, for the first time in the United Kingdom, the new laws will also implement a requirement to give notifications following some security breaches. Telecom companies and Internet service providers (ISPs) offering access to public networks will be covered by the obligation. They will have to notify regulators and in some cases those individuals whose personal data is affected. The regulators to be notified will be the UK communications regulator Ofcom and the Information Commissioner's Office (ICO). The government resisted calls to make the notification requirement more widespread across all industries, as is common in the laws of most American states.

Other Powers

The new laws will also include more powers for the ICO. In particular, the ICO will be given the power to serve information notices on third parties, to demand information from them that could help in an investigation. The government envisages that these notices will be served on telecom companies and ISPs to help identify spammers and direct marketing companies making unwanted telephone calls.

The Rest of Europe

The United Kingdom seems ahead of other EU countries in announcing its plans. The EU coordinating body for data privacy regulators, Article 29 Data Protection Working Party, published its report on the Directive "[Working Document 01/2011 on the Current EU Personal Data Breach Framework and Recommendations for Future Policy Developments](#)" on 5 April. It said of the data breach aspects of the Directive: "Currently, a minority of Member States are engaged in public consultation. Most of the Member States have draft texts, although the vast majority of them have not reached the status of proposed legislation. None of the Member States appear to have adopted legislation yet. . . . the above indicates that the implementation efforts have not reach an advanced

stage." The Article 29 Working Party says it believes that "an important number" of EU countries are unlikely to meet the 25 May deadline.

Of those EU countries that have published their plans, most intend to do the same with the security breach provisions as the United Kingdom and not extend the legislation beyond telecom companies and ISPs. Germany and Austria are the exceptions, as they already have wider data breach laws in place. The body to which breaches must be reported varies, with either the data protection authority (e.g., Estonia, Luxembourg, France), the telecom authority (e.g., Sweden, Finland) or both having power (e.g., Germany).

What Happens Next?

There is likely to be a period of continued uncertainty for anyone with e-commerce operations in Europe. Many of the new powers will fall to the ICO for enforcement. The ICO will release detailed guidance on the implementation of the cookie consent requirements prior to 25 May. It will also consult on its new information request powers. Vaizey said that he did not expect the ICO to take enforcement action in the short term against businesses and organizations, as details of the consent rules are fleshed out.

In the rest of Europe, the next month is likely to see more countries announce their proposals. Cookies have traditionally been one of the areas in which there is little harmony in Europe, and whilst there is hope that more countries take the United Kingdom's reasonable and balanced stance, that is by no means certain.

In addition to last week's announcement, the UK's Office of Fair Trading (OFT) also published its study last year of online advertising, as discussed in the 8 June 2010 *Duane Morris Alert*, "[UK to Focus Efforts on Regulating Online Advertising](#)." That study found that, although industry self-regulation was working to some extent, more could be done to provide consumers with full information about personal information collected online.

The OFT study warned that fair trading regulations also gave regulators the power to take action against corporations that do not fully disclose their information-handling

practices. For example, the [Consumer Protection from Unfair Trading Regulations 2008](#) give the duty to regulators to act when a consumer is deceived about the presence of cookies, even when the information they have been given is correct. The penalties under the UK legislation include fines or a prison term of up to two years.

The debate over the use of tracking tools on websites has been developing for some time. For any business selling or advertising online, or carrying advertising on its sites, transparency is likely to be the watchword.

For Further Information

If you have any questions 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](#).