ALERTS AND UPDATES

United Kingdom's New Laws on Cookies and E-commerce

May 23, 2011

The United Kingdom's new laws for Web cookies and e-commerce come into force on Thursday, 26 May 2011.

The new laws were announced in April after a consultation in which Duane Morris participated. 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 should also update their laws this week by the EU's 25 May deadline, although it seems that much of Europe is still not ready for the changes.

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 UK government's April response recognized 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." 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 argued for in Duane Morris' representations and an approach that 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 UK, the new laws will also implement a requirement to give notifications following some security breaches. Telecoms 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 (*e.g.*, Germany) having power.

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. On 9 May, the ICO issued its own guidance on the new laws. In its news release launching that new guidance, the Information Commissioner Christopher Graham said: "The implementation of this new legislation is challenging and involves significant technological considerations. . . . This advice is very much a work in progress and doesn't yet provide all of the answers."

In the rest of Europe, the next few months are 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 UK government's reasonable and balanced stance, that is by no means certain.

In addition to the new laws, 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 organizations that do not fully disclose their information-handling practices. For example, the Consumer Protection from Unfair Trading Regulations 2008 gives 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. Businesses may want to check their sites to work out where they are using cookies and what those cookies are doing. They may want to stop using unnecessary cookies, especially those sending data to third parties. Businesses may then work on ways of telling visitors to

their sites what is happening to 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 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.