Doing Business Online in Europe? New Law Will Require Customer Consent for Cookies

by Rafi Azim-Khan and Steven P. Farmer

An important new European Directive, which comes into force on 25 May 2011, will require companies with European customers to get informed consent from such visitors to their websites in order to use cookies. The Directive has pan-EU effect. The UK Information Commissioner's Office ("ICO") have recently published much-anticipated advice on how to comply with the new law from a UK perspective.

The Change In The Law

Under the EU's Privacy and Electronic Communications Directive (the "E-Privacy Directive"), the current rules on using cookies for tracking/storing information on users will change. Currently, a website operator has to:

- tell website users how they use cookies; and
- tell them how they can "opt out" if they object.

The new requirement is essentially that cookies can only be placed on computers where the user has **given their consent**. This change will come into force on 25 May 2011.

The only real exception to the rule is a website operator doing something that is "strictly necessary" for a service specifically requested by the user.

A number of question marks have surrounded what exactly this change will mean for both website operators and users. The ICO have now drawn up advice to help organizations think about the practical steps they **will need to take** to ensure compliance with the new law.

The ICO's Guidance

The ICO's guidance explains that the "strictly necessary" exception is a narrow one. However, it says that it may apply, for example, to a cookie a website operator uses to ensure that when a user of its site has chosen the goods they wish to buy and clicks "add to basket", the website "remembers" what the user chose on a previous page. In this case, the guidance suggests, consent would not be required.

Yet the guidance goes on to say that the exception would not apply, for example, just because a website operator decides that its website would be more attractive if it remembered users' preferences or it decides to use a cookie to collect statistical information about use of the website.

In terms of obtaining consent, the guidance states that information must be provided about a cookie before a cookie is set for the first time. Once consent is obtained, a website operator need not seek consent again for the same person each time the same cookie (for the same purpose) is used in the future.

How Is Consent Obtained?

Whilst the guidance recognizes that gaining consent "will, in many cases, be a challenge", it does set out ways in which consent could be obtained, explaining that "the more privacy intrusive your (i.e. the website operator's) activity, the more you will need to do to get meaningful consent".

For example, the guidance explains that consent can be obtained via the following methods:

- Pop-ups. A website operator could ask a user directly if they agree to a website operator putting something on their computer and if they click "yes", this would constitute consent.

- Terms and conditions. A website operator could alternatively make users aware of the use of cookies via the terms and conditions, asking a user to tick a box to indicate that they consent to the new terms.

- Settings-led consent. Consent could also be gained as part of the process by which the user confirms what they want to do or how they want the website to work, e.g., some websites "remember" which language version of a website a user prefers. If this feature is enabled by the storage of a cookie, then the website operator could explain this to the user and that it will not ask the user every time they visit the website.

It is worth noting, however, that the guidance does not purport to be exhaustive. The ICO states that they will consider supplementing the advice with further examples of how to gain consent for particular types of cookies in the future. It goes on to say that the examples listed are not intended to be a prescriptive list on how to comply, rather, that a website operator is best placed to work out how to get information to users and what users will understand. Each case will be facts-specific.

Do Website Operators Have to Comply With the Changes and Guidance?

Yes. The ICO have stated that if they were to receive a complaint about a website, they would expect an organization's response to set out how they have considered compliance. Examples would need to be shown. The ICO have stressed that the rules cannot be ignored.

In terms of UK enforcement, the ICO will shortly be issuing separate guidance on how they intend to enforce the change in the law, but it should be borne in mind, at the very least for now, that the ICO do

have the existing power to issue very significant "on-the-spot" fines for those found to have seriously breached data protection laws in the UK.

In terms of users in European countries outside of the UK, although we would expect the pending changes to be implemented in a very similar way across Europe, it is important to remember that other European regulators may interpret the changes to the E-Privacy Directive somewhat differently than the ICO.

The result is that compliance with the UK guidance when targeting, say, French customers, may not necessarily ensure compliance from the French regulator's perspective.

To be on the safe side, whilst compliance with the UK ICO's guidance will go a long way towards ensuring compliance throughout Europe, local advice should always be sought with respect to key European territories whose customers are targeted.

What Should Website Operators Do Before 25 May 2011?

Organizations using cookies on websites that are aimed at Europe should urgently (and in any case **before 25 May 2011**):

- check which territories their website is aimed at;
- check what type of cookies are in use;
- assess how intrusive the use of cookies is;
- decide on the best solution to obtain consent in each key territory; and
- consult with expert counsel to ensure that they are not made an example of by the relevant regulators come 25 May 2011.

Remember, enforcement of the new rules will not be on a "one size fits all" basis but rather very facts-specific to your cookies, website and users.

If you have any questions about the content of this advisory, please contact the Pillsbury attorney with whom you regularly work, or the authors of this alert.

Rafi Azim-Khan (bio)
London
+44.20.7847.9519
rafi.azimkhan@pillsburylaw.com

Steven P. Farmer (bio)
London
+44.20.7847.9526
steven.farmer@pillsburylaw.com