Cooley

June 20, 2011

New rules governing the use of website "cookies" were issued by the United Kingdom Information Commissioner's Office (ICO), effective May 26, 2011. These new rules require an "opt-in" system pursuant to which the use of cookies is only allowed after the user has given her consent. This opt-in system represents a change in the common practice of U.S. websites, which typically disclose the use of cookies in their privacy policies and provide users with the ability to "opt out" of such use. Although the ICO has included a 12-month lead-in period (through May 26, 2012) for organizations to develop ways to meet the new cookie requirements, it has also stated that companies subject to the new rules should be taking actions to bring themselves into compliance during this lead-in period. The U.K. rules implement 2009 amendments to the European Union's Privacy and Electronic Communications Directive (the "ePrivacy Directive").

Who is subject to the U.K. rules

Websites hosted in Europe are subject to the U.K. rules. The U.K. rules also purport to apply to websites that are hosted elsewhere if they target U.K. residents. As a result, U.S. website operators may be required to follow the new U.K. rules if they market their websites to U.K. residents or if U.K. residents are using their websites.

What technologies are covered

The U.K. rules apply to "cookies," which are small text files that a website automatically places on a user's computer when the website is loaded. There are many different types of cookies, including session cookies (which track a user's activity from page to page during a session so that the user does not have to re-enter information or selections); authentication cookies (which store logon credentials so that the user does not have to log on again after navigating to a different website); persistent cookies (which store user preferences for each successive visit to a site); and tracking cookies (which are used to collect analytic data on how an individual website is used and to record a user's activities across websites). The ICO Guidance on Changes to the Rules on Using Cookies and Similar Technologies for Storing Information ("ICO Guidance") states that the rules will also apply to similar technologies for storing information, such as Flash cookies, which are data files that are stored on a consumer's computer by a website that uses Adobe's Flash player technology.

Exception

The only exception to the U.K. rules is for cookies that are "strictly necessary" for a service requested by a user, such as the use of a cookie to facilitate the use of shopping baskets on websites, and the ICO Guidance makes it clear that the exception is to be interpreted narrowly: "The exception would not apply, for example, just because you had decided that your website is more attractive if you remember users' preferences or if you decide to use a cookie to collect statistical information about the use of your website."

How user consent can be obtained

The ePrivacy Directive suggested that browser settings could be used to obtain user consent. In other words, the website operator could identify to a user of its site that the user's browser is set up to allow cookies of types A, B, and C (but not type D), and such notice would signify the user's consent to use of cookies of types A, B and C. However, the ICO Guidance states that most browser settings are not currently sophisticated enough to allow a website operator to assume that a user has given his or her consent to allow the website to set a cookie based on the browser settings. The ICO Guidance also notes that some users will use an application on a mobile device, or other means than a browser, to access the website. As a result, the ICO's current position is that browser settings cannot be used to indicate the consent required by the U.K. rules. Instead, the U.K. rules provide that consent may only be obtained via browser settings where the consent is "signified by a subscriber who amends or sets controls" on the browser. The ICO has indicated that it intends to work with browser manufacturers to see if they can be enhanced to meet the requirements of the ePrivacy Directive and that it has formed a working group of representatives from the browser manufacturers to look at this in more detail.

The ICO Guidance offers a number of suggestions on how the required opt-in consent may be obtained, including the following:

- **Pop-ups and similar techniques**. The operator may use pop-ups or splash screens to obtain consent (although the ICO Guidance notes that this "might well spoil the experience of using a website if you use several cookies").
- **Website terms of use**. The consent can be included in website terms of use if the user is required to accept them by way of a positive action, such as checking "I accept," *before* the cookie is placed.
- **Settings-led consent**. The operator may incorporate consent as a part of the process by which a user confirms what she wants to do or how she wants the site to work. For example, if an operator offers a feature whereby the website "remembers" which version of the website the user wants to access, the operator could explain to the user that by allowing the operator to remember her choice, she is giving the operator consent to set the cookie.
- **Feature-led consent**. Some objects are stored when a user chooses to use a particular feature on a website, such as watching a video clip or when the website remembers what the user has done on previous visits in order to personalize the content that the user is served. In these cases, if the user takes some action to specify the features that he wants (e.g., by clicking a button), the operator can ask for the user's consent to set a cookie at that point if the operator makes it clear to the user that by choosing to take a particular action certain things will happen.
- **Functional uses**. Where an operator collects information about how people access and use its site via an analytic cookie, the operator must think about giving the user more details about what it is doing so that he can make an informed decision about whether to allow the collection of such information by the website. In this case, the ICO Guidance suggests that the operator might place some text in the footer or header of the web page which is highlighted or turns into a scrolling piece of text before the site places a cookie on the user's device. This could prompt the user to read further information (e.g., by way of a link to the operator's privacy policy) and make any appropriate choices that are available to him. The guidance also notes that the operator must make "absolutely clear" to the user if any information collected about website use is provided to a third party, as well as disclosing what the third party does with the information.

Third party cookies

The ICO Guidance notes that where a website displays third party content, such as an advertising network or a streaming video service, the third party may read and write its own cookies or similar technologies onto the website. The process of getting consent for these third party cookies is more complex, and may be the most challenging area in which to achieve compliance with the new rules. The ICO's view is that everyone has a part to play in making sure the user is aware of what is being collected and who is collecting it. The ICO notes that there are a number of initiatives to seek to ensure that users are given more and better information about how their information is used, and advises that any operator of a website that allows or uses third party cookies must make sure it is doing everything that it can to get the right information to users and that it is allowing users to make informed choices about what cookies are stored on their devices.

Enforcement

A serious breach (defined in another ICO Guidance on Enforcing the Revised Privacy and Electronic Communications Regulations as a serious contravention of the rules that is likely to cause substantial damage or distress) may result in penalties of up to £500,000 if it is deliberate, or the responsible person knew or ought to have known that a contravention would occur and then failed to take reasonable steps to prevent it.

Recommended actions

As noted, the U.K. rules purport to cover all website operators that target U.K. residents. Whether or not a U.S. website operator is determined to be covered by the U.K. rules, the trend toward requiring fuller disclosure and express consent, especially for targeted advertising cookies, is likely to be seen in the U.S. as well. For example, in its December 2010 report on consumer privacy, the FTC recommended that consumers be given the right to opt-in before tracking cookies are used. As a result, U.S. website operators should consider taking the following actions:

1. **Check what type of cookies and similar technologies you use on your website and how you are using**

them. You should determine which cookies you believe are "strictly necessary" and therefore will not require opt-in consent. You may also want to use this audit as an opportunity to stop using any cookies that are unnecessary or have been superseded as your site has evolved.
2. **Assess how intrusive your use of these cookies is**. The ICO Guidance notes that the more intrusive the use of cookies is, the more priority that an organization should give to considering changes to how you use it. In particular, the ICO notes that if a site is using tracking cookies, or allowing the use of tracking cookies, the operator will need to give more priority to getting meaningful consent.
3. **Update your privacy policy** to provide more specific information about the cookies you use on your website, the information that you collect, and the ways that you use this information.
4. **Decide what solution to obtain consent will be best for you** and implement that solution on your website.
5. **Review your contracts** with advertisers, advertising networks, providers of website and browsing statistics, and parties with whom you offer co-branded sites to ensure that they clearly set forth who is responsible for providing cookie notices and obtaining user consent where required.

Key Contacts

Adam Ruttenberg Washington, DC	aruttenberg@cooley.com +1 202 842 7804