BNA, INC.

PRIVACY & SECURITY LAW

BNA Employee-Owned Since 1947

REPORT

U.K. Privacy Commission Advice on New Cookie Rule: Likely to Cause Heartburn?

By Francoise Gilbert

Francoise Gilbert is the managing director of the IT Law Group, http://www.itlawgroup.com, a niche law firm that focuses on information privacy & security and cloud computing. She is the author of the two-volume treatise Global Privacy and Security Law, http://www.globalprivacybook.com, which covers the data protection laws in 62 countries on all continents and is published by Wolters Kluwer. She serves as General Counsel of the Cloud Security Alliance and as a Board Member of the International Technology Law Association. She can be reached at (1) 650-804-1235 and fgilbert@itlawgroup.com.

On May 9, 2011, the United Kingdom's Information Commissioner's Office (ICO) published an "Advice"[1] explaining the new rule for the use of cookie technologies for websites that are subject to U.K. laws. This rule results from the implementation of the *2009 Amendment to the 2002 EU's Privacy and Electronic Communications Directive* (also known as the e-Privacy Directive) into the U.K. laws. [2] It will amend Regulation 6 of the Privacy and Electronic Communication Regulations 2003 (PECR).

There are two basic requirements. Businesses and other entities are permitted to use cookie technologies only if the user of the site or application:

- has received clear and comprehensive information about the purpose for the cookie in question; and
- has given his or her consent to the use of the cookie.

[1] http://www.ico.gov.uk/~/media/documents/pressreleases/2011/cookies_regulations_advice_news_release_20110509.ashx

[2] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Devices, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, and Regulation (EC) No 2006/2004 on Cooperation Between National Authorities Responsible for the Enforcement of Consumer Protection Laws. The text of Directive 2009/136/EC available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:En:PDF.

 ISSN 1538-3423

What This Means for Companies

Companies that do business in the United Kingdom or are otherwise subject to the U.K.'s Data Protection Act, must promptly start considering ways to respond to the new requirements that result from the amendment of the PECR Regulations.

In brief, the new rule requires that users provide informed, affirmative consent to the use of almost any cookies that a website would wish to install on their machine. The restriction applies both for the installation of the cookie and the subsequent access to the information stored on the cookie. Except for a small category of cookies that are necessary for the proper operation of a site, or for offering a shopping-cart type feature, all other cookies, including those that are used for analytics purposes, require prior specific consent. Of course, flash cookies are also subject to the notice and consent requirement.

The only notable exception is that consent needs to be obtained only once. Thus, once a user has consented to the use of a particular cookie, there is no need to ask permission each time the website needs to access that cookie.

The ICO's Advice discusses several methods that might be used to implement the notice and consent requirement. The ICO envisions a sliding-scale approach, where the cookies that have the potential to be the most intrusive require the most specific and detailed notice. The ICO also suggests a tailored approach as opposed to the ''one-size-fits-all'' approach, commonly used currently in website privacy policies. The different models for expressing consent proposed by the ICO tend to be specific to a particular type of cookies, and the particular circumstances of its use.

As a first step in the implementation of the new rules, the ICO insists that website privacy statements should be revised promptly, to display more prominently those sections of the document that address the use of cookies. In a second phase, companies should conduct an audit of their practices, assess the different types of cookies to determine how intrusive they may be, and identify workable solutions to obtain users' consent. The ICO clearly states that it expects companies to promptly come up with a plan of action that shows that they have considered their obligations and that they have a realistic plan to respond to the new requirements and achieve compliance.

While there are many talks and negotiations throughout the European Union about how to implement the 2009 Amendment to the 2002 ePrivacy Directive, it is clear that the Advice prepared by the ICO clarifies the very confusing and controversial amendment. It provides specific guidance about the direction to take. As a result, it is also highly likely that this document will serve as guidance or a model to other data protection authorities who have been facing the same issues and need to implement the 2009 Amendment into their national laws. Thus companies that may not be subject to the U.K. laws, but otherwise do business in the European Union should read and understand the ICO's Advice, as a way to prepare for their obligations to comply with the national laws of the countries where they operate.

Overview of the New Rule for Cookies

The previous rule on using cookies—which was set out in Regulation 6 of PECR—required that users be informed about the existence of cookies, and be given the opportunity to refuse the storage of, or access to, the cookie information stored on their computers. Most companies provided the relevant information in their website privacy statement, and informed their users that, by changing their browser settings, they could arrange to block cookies.

Under the new rule, companies must still provide clear and comprehensive information about the use of cookies. However, the ***cookies may only be placed on a machine or device after the user or subscriber has given his consent.***

Exceptions

1 - Repeated uses

The consent need not be given each time. Under the new rule, if the same information is stored or accessed by the same entity, regarding the same user, on more than one occasion, the consent need to be obtained only once.[3]

2 - Transmission of communications

Notice and consent are not required for a limited number of cookie categories. Cookies that are required for the sole purpose of carrying out the transmission of communications over an electronic networks are exempt from the notice and consent requirement.[4]

3 - Cookies that are ''strictly necessary''

Cookies that are ''strictly necessary'' for the provision of a service requested by the subscriber or user are also exempt from the notice and consent requirement. According to the ICO's Advice, ''strictly necessary'' means that the use of the cookie must relate to the service explicitly requested by the user. The exception is narrow.

It would apply, for example, to a cookie that is used in e-commerce applications when a user has selected goods to purchase and clicks the ''add to basket'' or ''proceed to checkout'' button, to ensure that the site remembers what was chosen, and post the information on the check out page. On the other hand, as explained by the ICO, the exception would not apply, for example, to cookies used to track users to make the website more attractive because it remembers the users' preferences, or cookies that are used to collect statistical information about the use of the website.[5]

How Consent May Be Expressed

The rule allows consent to be signified by the user amending or setting controls on his or her browser, or by using another application or program to signify consent. However, as explained below, the ICO does not agree that using browser settings is currently a satisfactory method to express consent.

How to Implement the New Rules

According to the Advice, the ICO anticipates a phased approach to the implementation of these changes, and recommends that companies use the following steps:

[3] 2003 Regulations as amended, Section 6(3).
[4] 2003 Regulations as amended, Section 6(4)(a).
[5] Advice, page 3

  PVLR ISSN 1538-3423

1 - Identify what types of cookies are used and why

Companies should conduct an audit of their website to determine what cookies or data files are used and for which purposes. This would allow identifying which cookies are strictly necessary and might not need consent.

2 - Assess how intrusive these cookies are

The most intrusive cookies should be addressed first. For example, cookies that involve creating detailed profiles of an individual's browsing activity are intrusive—the more privacy intrusive an activity, the more priority should be given to getting meaningful consent

3 - Identify the best solution for obtaining consent

For each category of cookies or uses, the best method for gaining consent should be identified. The most privacy intrusive activities will require that the most information be provided to the user.

Different Methods for Obtaining Consent

The ICO's Advice provides a useful analysis of the different methods available to obtain the consent of the user. It opines against using browser settings, and instead recommends a more specific, targeted approach.

1 - Browser settings

The ICO recommends that organizations refrain from using browsers as a means for obtained consent because currently most browser settings are not sophisticated enough to allow a website to assume that the user has consented to the use of cookies. In addition, mobile application and other technologies do not rely on browsers.

2 - Pop ups and similar techniques

Pop-ups may be used to ask for consent. However, this practice may be annoying if numerous cookies are used. Thus, the ICO cautions that the use of pop-ups or ''splash pages'' may become frustrating if used too frequent.

3 - Terms and conditions

Consent could be obtained when a user first registers or signs up. In this case, the ICO recommends making users aware of the changes, specifically, that the changes refer to the use of cookies, then asking them to tick a box to indicate that they consent to the new terms. Specific information should be provided.

4 - Settings-led consent

Some cookies are deployed when a user chooses how the site works for them each time they visit the site, such as a particular language, the size of the text displayed on the screen, the color scheme, or a ''personalized greeting.''

In these cases, consent could be gained as part of the process by which the user confirms what she wants to do or how she wants the site to work. At that time, the user should be told that by allowing the website to remember her choice, she is also consenting to set the cookie.

5 - Feature-led consent

In the same manner as above where the user conducts a specific activity, there are circumstances where tracking technologies are stored when a user chooses to use a particular feature of the site such as watching a video clip, or when the site remembers what the user did on previous visits, in order to personalize the content that the user is served.

In these cases, the user is often invited to open a link, click a button or agree to the functionality being ''switched on.'' The ICO suggests asking for the user's consent to set a cookie at this point.

As for prior example, it should be made clear to the user that by choosing to take a particular action, certain things will happen that will be interpreted as the user's consent. If the anticipated use of tracking technology is complex or intrusive, it will be important to provide more specific information. In particular, as discussed below, users should be told whether some features are provided by a third party.

6 - Analytics and other functional uses

Many websites collect information about access to, and use of the site, and time spent on a page. While the ICO acknowledges that cookies used for analytics purposes might not appear to be as intrusive as others that might track a user across multiple sites, it nevertheless requires consent.

In this case, the ICO's Advice suggests that companies should make information about the use of analytics cookies more prominent, particularly in the period immediately following implementation of the new regulations. In addition, the ICO also suggests that website should give more details about the use of these cookies, such as a list of cookies used with a description of how they work—so that users can make an informed choice about what they will allow.[6]

If the information collected about website use is passed to a third party, this information sharing must be made absolutely clear to the user. Any options available should be prominently displayed and not hidden away.[7]

7 - Third party cookies

Finally, the ICO's Advice addresses the use of third party cookies. When a website displays content from a third party from an advertising network or a streaming video service, this third party may send its own cookies to the user. While the process of obtaining consent for these cookies may be more complex, the ICO opines that nevertheless the user must be made aware of what is being collected and by whom. This is a challenging area for which the ICO expects that more research will be needed to find workable solutions.

Next steps for the ICO

According to the ICO's press release, the ICO published the Advice in order to prompt organizations to start thinking about the practical steps they need to take to respond to this new requirement.[8] The press release also indicates that the ICO will provide additional content as innovative ways to acquire users' consent are developed.

Conclusion

The amendment to the U.K. rules comes into force on May 26. As a result of the implementation of this

[6] Advice, page 8.
[7] Advice, page 8.
[8] http://www.ico.gov.uk/%7E/media/documents/library/Privacy_and_electronic/Practical_application/advice_on_the_new_cookies_regulations.pdf

amendment into the U.K. laws, companies that operate websites in the U.K. must obtain informed consent from visitors to their websites and mobile applications in order to store and retrieve information on users' computers through cookies or similar tracking technologies. There are two basic requirements: providing clear and comprehensive information about the purpose for each cookie; and obtaining the prior explicit consent to the use of the cookie. While the ICO envisions a ''sliding scale'' approach, where the cookies that have the potential to be the most intrusive require the most specific and detailed notice, it also expects companies to delve promptly into implementation of the rule.

At a minimum, companies should promptly update their website privacy statements to clearly and conspicuously explain how cookies are used. In a second phase, companies should conduct an audit of their practices, assess the different types of cookies to determine how intrusive they may be, and identify workable solutions to obtain the requested consent.

The ICO has indicated clearly that it intends to enforce the new rule. While it concedes that full implementation will take time, the ICO wants companies to make every effort to start working on their use of cookies, and be prepared to provide tangible proof of their efforts to comply with the new rules.

  PVLR ISSN 1538-3423