

Articles

EU Requires Consent Before Cookies Can Be Placed

Dean W. Harvey and Ignacio Hirigoyen
IP and Technology Developments - July 2011
July 21, 2011

On May 26, 2011, the 2009 amendments¹ to the e-Privacy Directive² (the "Directive") regulating the use of internet cookies in the European Union ("EU") went into effect. The Directive, as amended, requires website operators and advertising companies falling within the legal jurisdiction of the EU to gain explicit consent before placing any cookie on users' machines.

What Is Changing?

Before the Directive was amended the EU only required companies to inform users that cookies were utilized and to supply users with information regarding how to "opt out" if the users objected to the cookie being created on their device. Sites often include in their privacy policies information regarding the use of cookies and the ability by users to "opt out" of the placement of such cookies.

Generally, the Directive only permits cookies to be placed after users have given consent (an "opt in" option). However, the Directive would not require consent for certain cookies that are "strictly necessary" to provide the services requested by a user. For example, if a user accesses a website to purchase an item, before proceeding to checkout, the site will be able to "remember" what was chosen on the previous page in order to be able to perform the transaction. These are known as "Session Cookies," and no consent shall be required for the use of this type of cookie.

How Should Companies Prepare for the New Requirements?

The first step in this preparation should be to assess how website(s) of a company under the jurisdiction of the EU work. This can be done by:

1. Performing a comprehensive audit of the company's website(s) to identify what type of data files and cookies are stored on users' devices when they visit the site, and which of those cookies are necessary to their business and might require consent, and also identify the Session Cookies that will fall outside the legislation.
2. Cleaning up their web pages and discontinuing the use of cookies that are outdated or that have been rendered obsolete because of changes to the company's website.
3. Determining if the website displays content from third parties (e.g., from an advertising network or a streaming video service). Such third parties may read and write their own cookies or similar technologies onto a company's users' devices. The process of getting consent for these cookies will be more complex and everyone should make sure that the user is aware of what is being collected and by whom.

Once a company has identified the type of cookies it places on its visitors' devices, it can begin to devise the plan it will use to require visitors' consent that best fits the company's business model and needs.

Obtaining Users' Consent

Below are implementation strategies that may assist in achieving compliance with the new legislation.

1. Browser Settings

Browser settings could be one possible mechanism to get the consent of users. When users visit a company's website, the website would identify whether a certain type of cookie is enabled in the users' browser. If users' browsers enable the type of cookies used by the company's site, it may be argued that consent was already granted. However, it is unclear whether this type of browser-enabled consent can satisfy the stricter requirements of the new legislation.

Articles

Another potential problem with this alternative is that many browsers are not sophisticated enough to support this functionality and not everyone will access a website through up-to-date browsers. Thus, this approach does not appear likely to lead to full compliance.

2. Pop-ups

Using pop-ups to ask for consent may initially seem like an easy option for complying with the new legislation since the company would be asking the user directly for their consent to install a cookie on their device. The drawback with this strategy is that pop-ups are unappealing to web users, and can be blocked.

3. Execution of an Agreement

There is no reason why consent for the purposes of complying with the new legislation cannot be gained through electronic execution of an agreement, including other website terms and conditions. However, it is important to note that changing a website's terms of use alone to include consent for cookies would not satisfy the requirements of the legislation, even if a user had previously consented to the terms. To satisfy the new rules on cookies, the company has to make users aware of the changes to the terms and conditions and specifically that the changes refer to their use of cookies; then the company needs a positive indication that users understand and agree to the changes, such as checking a box. The key point is to be upfront with the users about how the website operates and making certain that the users are fully informed.

4. Consent Based on Certain Settings

Certain sites deploy cookies depending on users' choices. For this type of cookie, consent may be obtained as part of the process by which users confirm what they want to do or how they want the site to work. For example, some websites "remember" which version a user wants to access, such as version of the site in a particular language. If this feature is enabled by the storage of a cookie, then the company provides notice of this to the user and the user consents by establishing the settings. This approach would only apply to features for which the company would explain to users that the site can remember certain settings they have chosen (i.e., language, font, background, music on, etc.).

5. Consent Based on Certain Features

After users choose a particular feature on a website, such as playing a video, the site will remember what that user has done on previous visits in order to personalize that user's content. In these cases, consent will be acquired by presuming that by the user taking certain action, the user is telling the webpage what he/she wants the site to do (either opening a link, clicking a button or agreeing to the functionality being "switched on"), and the cookie will be placed. Companies using this strategy need to make clear to users that by choosing to take a certain action the company is obtaining consent from the user. The more complex or intrusive the activity the more challenging it will be to fully inform the user.

Conclusion

The amended Directive moves the EU from an "opt out" to an "opt in" model for obtaining consent before placing cookies on a user's device. Compliance with this requirement will likely present significant challenges. In order to comply, companies need to understand what cookies their sites place, and establish a strategy for obtaining consent from users in the EU.

1. Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 OJ L 337 amending the e-Privacy Directive.

2. Directive 2002/58/EC of the European Parliament and of the Council of 12 July concerning the processing of personal data and the protection of privacy in the electronic communications sector of 12 July 2002 OJ L 201/37.

For more information, please email IPandTech@andrewskurth.com.

Articles

Click the links below to contact the authors of this article.

Dean Harvey or Ignacio Hirigoyen

Other articles from this issue of *IP and Technology Developments*.

- Patents by the Numbers
 - Recent Cases Should Make Software Licensors Review Their Distribution Methods and License Terms (and They May Even Make Us Look at Open Source Licenses in a Different Way)
 - On Your .Mark, Get Set, GO! — ICANN Opens the Internet to Unlimited Generic Top-Level Domains
 - The New “Willful Blindness” Standard for Inducing Patent Infringement
-

Download a PDF of the entire issue.

Click here to subscribe to future Andrews Kurth alerts.