Using Cookies on the World Wide Web? U.S. Companies Should Pay Heed to Changing EU Law

May 12, 2011

Web "cookies" are crucial to the convenience of the Internet. These small data files store passwords and user preferences and track users' Internet movement, allowing for targeted and affiliate marketing. Cookies reflect the tension between ease-of-use and privacy found in online commerce. In the United States and under the prior law of the European Union, users can "opt out" of receiving cookies, usually by adjusting their browser settings.

Under the EU's new e-privacy directive, the default rule will be that a web site must ask users to "opt in" *for each first-time use of a cookie*. Imagine incessant pop-up windows asking, "Do you accept this cookie?" At issue is whether European regulators will give a broad (and practical) reading to the exception to this new "opt-in" rule. Although the EU is not expected to begin immediate enforcement of the directive, any business with European visitors to its web site should review its "cookie policy" now.

What Happened

The EU approved the Privacy and Electronic Communications Directive in 2009, making it **effective May 26, 2011**. Under the directive, web sites must get clear, informed and "explicit consent" by notifying visitors each time a new cookie is placed, *unless* that cookie is "strictly necessary for the legitimate purpose of enabling the use of a specific service explicitly requested." What does this exception mean? Web site operators and online advertisers have been awaiting clarification and the United Kingdom's Information Commissioner's Office (ICO) attempted to provide it earlier this week with a ten-page published guidance, found here.

The ICO suggests the exception is narrow, and believes that in most instances users will have to "opt in" to a site's individual cookies. The ICO would apply the exception to limited situations, such as a user clicking the "proceed to checkout" button. No opt-in request would be required for the cookie "remembering" the user's items for purchase, says the ICO, because the cookie is "strictly necessary" for the purchase to go forward. The ICO rejects use of the exception "just because you have decided that your web site 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." Of course, these are the reasons most businesses use cookies today.

The ICO advises that changing the terms-of-use language for a web site from "opt out" to "opt in" for cookies is not good enough. It admits, however, that most browser settings are presently not sophisticated enough to provide for a multi-tiered permission tickbox upon visiting a site.

What it Means

Web site operators should know what cookies, including any third party cookies, attach to users at their site. They should provide transparent disclosure of their use of cookies. If the web site has limited interaction with EU users, the operator can likely continue to rely on the "opt-out" method for the time being. In the end, there is a strong likelihood that industry self-regulation measures or new, more sophisticated "opt-in" election technology will solve this problem. Still, businesses that deal with the EU need to track this issue closely.

What You Should Do

If you have any questions or concerns regarding the new EU cookie directive, or other privacy risks, compliance, or litigation, please contact your Lathrop Gage attorney or the attorney listed above.