Davis Wright Tremaine LLP

Six Tips for Compliance with Europe's New Cookie Rules

By Robert F. Stankey and Adam Shoemaker

July 06, 2011

While the European Union's deadline for implementing new cookie rules has passed, substantial uncertainty remains about what organizations should do to make their online activities compliant. In this advisory we offer six practical tips for dealing with the uncertainty.

Background

The EU adopted the Citizens' Rights Directive ("Directive") in 2009 as part of a package of changes to update communications regulation. The Directive imposes new consent requirements on websites that use cookies, including potential limits on the use of online tracking for behavioral advertising. While the Directive's implementation deadline was May 25, 2011, only a handful of European countries have completed their transposition of the new rules into national law.

EU member states have significant discretion to determine how they will implement the new rules, and many governments have delegated the interpretation and application of these rules to their national or regional data protection authorities. Consequently, even where legislation has been adopted, detailed implementation guidance will be needed. Given the broad scope of possible obligations under the Directive and the potential for a variety of interpretations of its rules, organizations operating websites or providing services over the Internet will need to assess their potential compliance obligations and monitor how key jurisdictions are interpreting the requirements.

The Directive amends the EU's earlier e-Privacy Directive, which was adopted in 2002. One of the significant implications of the new rules is the requirement that a website user give consent to the use of cookies after having been provided information about cookie use. Under the old rules, providing the ability to opt out of cookies was sufficient, and notification of such a policy could be incorporated into a website's main privacy statement. If opt-out is no longer allowed, what form of an "opt-in" consent is required? Can Web browser settings satisfy the requirement for consent?

A single interpretation of the new cookie consent requirement has not emerged. The coordinating group for European data protection regulators, the Article 29 Working Party, issued an opinion in June 2010 that advocates a strict interpretation of an opt-in requirement. Under the most rigorous application of an opt-in cookie system, a website visitor would be required to affirmatively accept the cookie through a pop-up screen or similar splash page before entering a website. This type of application would have significant implications for European website operators.

There is good reason to believe that few, if any authorities will implement the opt-in rule in the manner advocated by the Working Group. First, the new rules provide some leeway on the type of consent required, stating that consent is not required when a cookie is "strictly necessary" for a service that has been requested by a customer, and declining to define the required standard as "prior consent." Second, the Directive permits the user to express consent through browser settings, opening the possibility that consent requirements could be satisfied by a user's declared preference to accept cookies through browser settings.

More importantly, because each EU member state will have some flexibility in interpreting and implementing the new rules, each may choose to impose requirements that are less drastic than the Working Group recommendation. As an example, the U.K., recognizing the importance of a streamlined user experience on websites, has rejected a strict opt-in system based on "prior consent" and has announced a more flexible interpretation focused on "informed consent."

According to guidance published by the U.K. Information Commissioner's Office (ICO), "informed consent" can, among other ways, take the form of browser settings—even a default setting to accept cookies that has not been changed by the user (assuming adequate and prominent disclosures have

been provided). The ICO's approach gives the U.K. flexibility to adjust its interpretation of the Directive's requirements on an ongoing basis. This will provide the U.K. and states that adopt similar policies the ability to adjust enforcement as browser technology advances and behavioral marketing methods evolve.

Because each member state may implement the rules differently, and because a significant number may adopt a flexible, adapting enforcement regime like that outlined by the U.K., website operators in Europe should prepare to face requirements along a spectrum of possible interpretations of the Directive's opt-in provision. These may range from a gradual shift toward browser-based opt-in systems at one end and, at the other extreme, immediate calls for affirmative statements of consent by users for each individual website.

Compliance tips

In the short term, many organizations will need to strike a balance and look at practical ways to minimize potential problems under the new rules. With that in mind, we offer the following tips:

1. Decide what rules apply. The new cookie rules may not apply to your organization. Companies based in Europe and websites hosted on servers located within the European Economic Area will need to comply with the new rules. Websites hosted outside the EEA are probably, as a strict matter of law, also subject to the new rules if they are used by European residents. However, organizations with no meaningful activities or presence in Europe are unlikely to be the subject of enforcement action given the difficulty that regulatory authorities have in pursuing website operators with no local assets. Similarly, online services that are targeted at only a few European countries can focus on complying with only those countries' cookie rules. (Remember the cookie rules are not based on EU data protection law—consent is required regardless of whether personal data is collected from a user.)

2. Audit your use of cookies. Organizations that are likely to be subject to the new rules should find out how they are currently using cookies. A "cookie audit" should include an examination of what types of cookies are used and for what purpose, how the information is being processed, and what third parties have access to cookie information or drop cookies via your website. Cookies that are no longer needed should be eliminated from websites. The audit should also assess whether cookie-related information is being used in more ways than is necessary and whether third-party cookies should be used in a more limited way.

3. Focus on certain cookies. Regulators are unlikely to start an investigation (or receive complaints from users) about an organization's use of cookies for many common internal purposes, such as session cookies and website analytics that use first-party cookies. Cookies that are "strictly necessary to provide services" are expressly exempt from the consent rules. Even if they do not qualify as cookies "strictly necessary" for a service, cookies that are used internally to track site usage or otherwise make improvements to a website and its content are unlikely to pose a compliance problem. Instead, organizations should focus on the use of cookies for purposes unrelated to their websites and on third-party cookies.

4. Add consents to registrations. Organizations that require users to register to access certain online content or features should add an explicit consent to the use of cookies. This can be done in various ways, but a clear "check-the-box" opt-in consent is the optimal solution. If the consent is meant to be collected at the same time that users agree to the terms of service or a privacy policy, care should be taken to make sure a statement about the use of cookies is clearly visible, such as near the "I agree" check-box or button, and also include mention of how users can opt out of cookies in the future.

5. Make cookie disclosures more prominent. Many websites will not have an opportunity to ask users to register and give an explicit consent to cookies. Some organizations may be willing to put on their main website landing page a prominent statement (such as a pop-up consent window or a simple banner that does not require a click-through) disclosing the use of cookies. However, we expect that most website operators will find this difficult to do. Consequently, other disclosures, such as privacy policies and terms of use, will become the principal way that websites will be able to demonstrate they have obtained consent to the use of cookies. Such policies will need to be rewritten to include clear language about

consent to cookie use (and how to opt out of cookies in the future) and make such statements more prominent rather than buried in fine print. Disclosures about the use of third-party cookies, and how browser settings can be used to manage their use, will also need to be reviewed.

6. Monitor developments. The EU's adoption of the Directive is only the beginning of a process in Europe. Further steps need to be taken in many countries to complete implementation of the new rules, and regulators will continue to interpret how the rules should be applied in practice. Changes in browsers and smartphone platforms will also influence the evolution of the rules. Regulators are looking to the major browser makers to provide new ways for users to provide informed consent when online. In particular, organizations will need to consider the "Do Not Track" capabilities that are being added to browsers.

* * *

It is hoped that EU data protection authorities will allow organizations to come into compliance with the new rules over the next several months, given the continuing uncertainty about how the rules should be put into practice. For example, the U.K. has informally adopted a one-year phase-in period in which it does not expect to impose penalties for noncompliance. Nevertheless, companies with significant online activities need to take steps now to ensure that their users are informed about their use of cookies.

How can we help?

DWT's privacy lawyers have been following the development of the new rules for many years, having helped clients lobby in Brussels when the e-Privacy Directive amendments were still being negotiated. We work with clients in evaluating the risk areas in their use of cookies, structuring practical approaches toward compliance, and revising privacy policies and website registration processes to meet the new rules' notice and consent requirements. We welcome your inquiries.

Bob Stankey is a partner in DWT's Washington, D.C., office and qualified to practice law in the U.K. and the U.S. Adam Shoemaker is an associate in DWT's Washington, D.C., office. They can be reached at bobstankey@dwt.com and adamshoemaker@dwt.com.