



PRIVACY & SECURITY LAW



REPORT

Reproduced with permission from Privacy & Security Law Report, 10 PVLR 752, 05/16/2011. Copyright © 2011 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

How to Do Cookies Without Clear Directions: What Organizations Can Do to Prepare for the Looming Implementation of the ePrivacy Directive



BY **KARIN RETZER** AND **JOANNA LOPATOWSKA**

The amendments to the ePrivacy Directive¹ made at the end of 2009 mark a shift toward user consent for tracking cookies and similar technologies.

¹ 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 amended by Direc-

Karin Retzer is of counsel to Morrison & Foerster, Brussels, where her practice focuses on electronic commerce and data protection, technology licensing, and intellectual property law. Joanna Lopatowska is an associate in the Privacy and Data Security Group in Morrison & Foerster's Brussels office.

Cookies are small text files that are placed on a user's computer when visiting a website. When the user revisits the site, his or her browser returns the information collected by and stored in the cookie to the site, providing a "memory" of what the user did on the site. This information may be used for security purposes, or to facilitate navigation, or to personalize the user experience while visiting a site, e.g., by recording products in an online shopping cart, or storing language preferences. Cookies may also be used to facilitate the creation of user profiles based on Internet navigation or user segmentation for purposes of targeted advertising campaigns.

Under Article 5(3) of the amended ePrivacy Directive, users must be provided with "clear and comprehensive information" about the storage of information, or access to information stored, on their terminal equipment, and users must provide their "specific" and "freely given" consent. What is clear from the new language is that consent is required, and thus the mere right to object is insufficient. The different language versions of the text do, however, give no clear indications as to whether notice and consent should be provided before cookies are set, and it is unclear what type of consent is required. In particular, it is unclear whether consent must be explicit (opt-in), or whether implied or tacit consent would be sufficient.

In light of these ambiguities, industry stakeholders have raised concerns about the ePrivacy Directive's impact on electronic services. To date, the approaches to implementation across Europe represent a multitude of different requirements and interpretations. In addition, the implementation process is slow, and the May 25,

Directive 2009/136/EC of the European Parliament and of the Council of 25 November [2009] OJ L 337.

2011 deadline is not likely to be met by most EEA Member States.²

Although it is not yet possible to fully assess what shape the implementation legislation will take, below we summarize transposition of the ePrivacy Directive to date, and provide suggestions for organizations on how to modify policies and practices in order to prepare to face the new requirements.

1. Who must comply?

One of the fundamental questions concerning the interpretation of Article 5(3) is its scope of application: who must comply with the requirements? In general terms, the ePrivacy Directive applies to “providers of publicly available electronic communications services.” But there is no clear indication on how to interpret these terms in the context of services that use cookies; national legislation or guidance from data protection authorities will need to clarify the wording. EU-wide implementation of the ePrivacy Directive does not mean harmonization of rules; the types of entities covered by the broad understanding of such “providers” will not be the same in all Member States.³

Recent guidance from the U.K. Information Commissioner’s Office (“ICO”) indicates that all U.K. businesses and organizations running websites in the U.K. should comply. Documentation in Poland only makes vague references to “internet service providers.” The French data protection authority, the CNIL, understands that all “data controllers” who control the collection and use of information through cookies or similar technologies are covered, ranging from web publishers, web analytics providers, online advertising firms, and advertising network providers. German guidance places requirements squarely on web publishers, as well as analytics and advertising network providers. The Article 29 Working Party (“WP 29”), the EU advisory body composed of the national EU data protection authorities, finds that the obligations in Article 5(3) apply to advertising network providers, but that web publishers (websites cooperating with network providers) have limited obligations as well.

In addition, national legislators have entered into discussions with browser manufacturers regarding modifying default settings so that cookies would be rejected automatically; cooperation between the different parties will be crucial.

Despite these different interpretations, it is clear that website operators will not be able to shift the compliance burden to service providers such as advertising

networks, behavioral advertising, web analytics, or other services.

2. Which technologies are covered?

Article 5(3) of the ePrivacy Directive applies to the storage of or access to “information” stored in the device of a subscriber or user. This means the use of cookies and similar technologies for storing information, such as Locally Stored Objects (commonly referred to as “Flash Cookies”).

In order to answer the question of how to comply with Article 5(3), it is further necessary to examine the purposes for which cookies are used. Article 5(3) distinguishes cookies that are “strictly necessary” to the operation of a website or its services from other types of cookies that can be considered as merely complimentary. Cookies that are “strictly necessary” to provide the service requested by the user will be exempt from the requirements set out in Article 5(3).

What is meant by “strictly necessary” has not been explained, and therefore Member States will need to provide their own interpretations. Such “strictly necessary” cookies may be understood as cookies aimed at allowing users to better navigate websites and manage their accounts, for example, by storing passwords and language preferences. The CNIL reportedly considers that web analytics could be covered by this exemption. The Düsseldorf Kreis, the assembly of the German data protection authorities, does not consider cookies used for web analytics to be covered by the exemption. In the U.K., guidance suggests that the exemption should be interpreted narrowly and may only cover the use of cookies with respect to “traditional” online services, such as shopping or banking.

Users must provide their consent to the deployment of cookies used for other purposes. Such cookies may be used to track and analyze users’ online behavior, create user profiles, etc., most often in the delivery of behavioral advertising and analytics services. Other cookies may be used to track user behavior and merge that data with other user information with a view to improving services. Cookies may also be used to deliver a specific type of targeted advertising that distinguishes between prospects and customers, or to measure online marketing activity.

3. Notice and consent: In search of a pan-European standard

As stated, there is currently no general approach to interpretation of the notice and consent requirement will be; the interpretations of Member States, data protection authorities, and the EU institutions vary. The Communications Committee set up to advise Member States on implementation (composed of Member State and European Commission representatives) made an attempt to clarify the concept of consent. However, while it explained in detail what informed, specific, and freely given consent is, the Committee did not explicitly state that consent should be prior and opt-in. Instead, the Committee seems to suggest that browser settings or other application settings could be sufficient as a form of consent.⁴

⁴ Communications Committee, Working Document on Implementation of the revised Framework – Article 5(3) of the ePrivacy Directive, COCOM10-34 final (Oct. 20, 2010).

² The European Economic Area (EEA) comprises the Member States of the European Union, as well as Iceland, Liechtenstein, and Norway. The 27 Member States of the European Union (EU) as of January 1, 2007 are: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, the Netherlands, and the United Kingdom.

³ For the purposes of this article, the “providers of publicly available electronic communications services” that could be covered by the ePrivacy Directive, i.e., companies operating online by operating websites or online retailing, content providers (web publishers), providers of online behavioral advertising and web analytics services, and advertising network providers, are referred to collectively as “web operators.”

In contrast, for cookies used in online behavioral advertising, the WP 29 strongly advocates an opt-in consent requirement, stating that users must affirmatively consent to cookies before cookies are placed on their computers.⁵ The WP 29 stresses that informed consent can only be obtained if prior information about the placing and purposes of the cookie has been provided. The WP 29 states that obtaining consent via browser settings would only apply in “very limited circumstances,” and would have to conform to the general requirements of the EU Data Protection Directive.⁶ The WP 29 considers that the average user is not aware of the tracking of their online behavior, the purposes of the tracking, or how to use browser settings to reject cookies, even if the information is included in a privacy policy.

The WP 29’s role is advisory and aims to guide Member States in their implementation of the ePrivacy Directive. In practice, however, the WP 29’s position will not lead to a unified EU-wide approach, and some Member States have already adopted or are moving towards less restrictive legislation.

4. Different Member States’ approaches

The Member States have until May 25 to transpose the ePrivacy Directive into national law.⁷ Only days from the deadline, most Member States have still not completed implementation. One of the biggest concerns is that Member States will implement the cookie requirements in different ways. This would lead to myriad requirements across the EU, with some Member States following the WP 29 position and imposing “hard” opt-in consent, and others choosing a more pragmatic, business friendly approach by allowing user consent through browser settings. Currently, the default settings of major browsers generally allow cookies, and as such the ePrivacy Directive’s impact on electronic communications service providers could be relatively minor. Browsers may need to be adapted to better inform users and to be more user-friendly in general, shifting some of the practical burden from the web operators setting cookies to those creating and offering browsers.

Below we provide an overview of the approaches to implementation in key Member States:

■ **France:** In France, a relatively restrictive draft law to implement the ePrivacy Directive was adopted by the Senate in March 2010,⁸ but the draft has not been approved by the National Assembly. One year later, a law was adopted to enable the French government to legislate by ordinance to transpose the ePrivacy Directive into French law.⁹ The government has presented a draft ordinance,¹⁰ Article 37 of

which requires data controllers to clearly and comprehensively inform users, and obtain their consent for any use of cookies or similar technologies. There is no need for consent to be express; implied or tacit consent may suffice. An exception is provided where the cookies are used to facilitate a communication, or are “strictly necessary” to deliver a service expressly requested by the user. The CNIL has given indications that browser settings could provide one solution to obtaining prior notice and consent for cookies. But the CNIL has also asserted that most browser settings are not detailed or comprehensive enough to sufficiently inform the user about the different types of cookies set. Rather, users should be informed through an easily accessible notice, for example via a clearly displayed notice outside the privacy policy. It would be the responsibility of the web publisher, and not the web analytics provider, to provide notice.

■ **Germany:** Although case law is inconsistent, the German data protection authorities view any use of IP addresses as processing “personal data.” Based on this wide interpretation of “personal data,” the authorities already require web publishers to obtain prior notice and opt-in consent for the use of tracking technologies under general data protection laws. In late 2010, the Düsseldorf Kreis published guidance on the use of web analytics which states that user notice and opt-in consent is required unless IP addresses are truncated.¹¹ The amendments to the ePrivacy Directive will therefore not likely lead to significant changes in German legislation; what has changed is the attitude of the German data protection authorities. The German authorities are now much more active in enforcing their initial interpretation of “personal data” and regularly audit websites, but to date no fines have been imposed on any non-compliant sites.

■ **United Kingdom:** U.K. implementation legislation, the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 (“Regulations”), which should come into force May 26, copies the wording of Article 5(3).¹² Although there is a reference to browser settings as a means to obtain consent in the text, according to a government communication¹³ and guidance from the ICO, current browser settings that accept cookies by default are not sufficient for consent. The government therefore intends to work with browser manufacturers with a view to enhancing browser settings. The government has also expressed its support for an industry initiative to provide information on the use of cookies via an easily recognizable internet icon.¹⁴ Such an icon would link to information about: each specific Internet advert; the advertiser; the server; by whom the advert has been selected; and an option to refuse those and other cookies (including an option to refuse all cookies from that server). On May 9, the U.K.’s data protection authority, the ICO, issued a guidance paper on the new framework for cookies.¹⁵ It stresses that web-

⁵ Article 29 Working Party, Opinion 2/2010 on online behavioral advertising, WP 171.

⁶ Directive 95/46/EC of October 24, 1995 on the protection of individuals with regard to the processing of personal data and on free movement of such data [1995] OJ L 281/31.

⁷ The EEA Member States Iceland, Liechtenstein, and Norway are bound to implement most EU legislation—including the e-Privacy Directive—under Article 7 of the European Economic Area (EEA) Agreement.

⁸ Proposition de Loi N° 2387 visant à mieux garantir le droit à la vie privée à l’heure du numérique.

⁹ Loi N° 2011-302 du 22 mars 2011 portant diverses dispositions d’adaptation de la législation au droit de l’Union européenne en matière de santé, de travail et de communications électroniques.

¹⁰ Full text of the draft ordinance is available, in French, at <http://op.bna.com/pl.nsf/r?Open=dapn-8gqj9j>.

¹¹ Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 26/27, November 2009 in Stralsund.

¹² The text of the amendments to the UK Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 is available at: <http://www.legislation.gov.uk/ukxi/2011/1208/contents/made>.

¹³ The government’s statutory response to its stakeholder consultation is available on the Department for Culture, Media, and Sport website at <http://www.culture.gov.uk/publications/8048.aspx>.

¹⁴ See IAB Europe’s website for further information: <http://www.iabeurope.eu/news/self-regulation-framework.aspx>.

¹⁵ Information Commissioner’s Office, *Changes to the rules on using cookies and similar technologies for storing information*, available at http://www.ico.gov.uk/~media/documents/library/Privacy_and_electronic/Practical_application/advice_on_the_new_cookies_regulations.pdf.

site owners should seek consent for using cookies through other means than current browser settings or terms and conditions, for example through footer language on web pages, pop-ups, or language provided to users requesting particular services or features. The only exemption is for cases where the use of cookies is “strictly necessary” for a service requested by the user. In the paper, the ICO states that it expects all “UK businesses and organizations running websites in the UK” to conduct a comprehensive audit, and to “set out how they have considered the points above and [ensure] that they have a realistic plan to achieve compliance.”

- **Finland:** Finland appears to be following the U.K. government’s line of thinking. The Finnish Parliament has already adopted amendments to Finland’s Act on the Protection of Privacy in Electronic Communications.¹⁶ The amendments require user consent, and provide that such consent can be obtained through browser settings. In addition, the new law holds that browsers should be “user friendly” and thus provide a legitimate method through which user consent can be obtained. The amended Act will enter into force May 25, 2011.

- **The Netherlands:** In the Netherlands, the discussions are still ongoing. After much debate, the most recent draft bill¹⁷ seems to allow for opt-out consent through browser settings in certain situations, and acknowledges that it would be impractical to request opt-in consent each time a user visits a website that deploys cookies. The Dutch data protection authority has voiced strong opposition to the draft, arguing in favor of opt-in consent. The Dutch Parliament is now examining the draft bill, and will decide which approach to follow.

- **Ireland:** Irish legislation is far from being finalized and it remains unclear how the Irish authorities will interpret and implement the ePrivacy Directive. Although valid until new legislation is adopted, the present provision to provide opt-out via a privacy policy is unlikely to be maintained. However, the amendments proposed by the Department of Communications suggest that enhanced browser settings could be used to express user consent. The Office of the Irish Data Protection Commissioner recently suggested delaying transposition of the ePrivacy Directive — or at least Article 5(3) — for a period of around six months. This would allow industry and regulators to continue their discussions on how to best address the consent requirements.

- In most other Member States, legislation is still at the drafting stage, and implementation is unlikely to meet the deadline. In **Belgium**, draft legislation is expected to be submitted to Parliament soon. In **Poland**, the response to the government’s public consultation is still being reviewed and discussions continue regarding the specific form of consent; the Ministry of Infrastructure’s guidance on its draft legislation stipulates a requirement for opt-in consent. In **Spain**, draft legislation has been strongly influenced by the data protection authority’s reading of Article 5(3), which is closely aligned with that of the WP 29. However, the timetable for implementation and how legislation will be worded remain unclear.

5. The cross-border dilemma

Amongst all the discussion and differing implementation of the ePrivacy Directive, one crucial question remains unanswered: how will organizations operating in multiple jurisdictions determine applicable law?

¹⁶ Act on the Protection of Privacy in Electronic Communications PPEC No. 516/2004, amended by Act No. 365/2011 of April 8, 2011.

¹⁷ Draft bill No. 32 549 of November 8, 2010 amending Telecommunications Act of October 19, 1998.

Under the current data protection rules set forth by Article 4 of the EU Data Protection Directive, the principal criterion for determining applicable law is the place of establishment. However, if the provider is not established in the EEA but makes use of the “equipment” located there to process data, the relevant Member State’s law will apply. According to the Communications Committee, a user’s personal computer should be viewed as equipment.¹⁸ Therefore, websites hosted on servers outside of the EEA but providing services there will likely be covered by the cookie consent requirement.

In its December 2010 Opinion on applicable law,¹⁹ the WP 29 also argues that where data are collected by multiple entities in a number of EEA Member States, data controllers must comply with the rules applicable in each Member State where data collection takes place.

6. In practice: How to comply with Article 5(3)

How can organizations prepare to face the new requirements? How should they modify policies and practices? Unfortunately, given the delay in implementation, there are no clear directions yet. Worse, most Member State laws are likely to reflect the vague wording of Article 5(3), and further guidance from national data protection authorities may be required. Also, technical solutions that may satisfy requirements, such as “enhanced” browser settings, or an industry-wide Internet icon, are only in their infancy.

This leaves organization in a difficult situation. The U.K. government has stated quite clearly that, while it does not expect perfect compliance from organizations, given the legal and technical difficulties, it does expect organizations to actively work toward better compliance: “*The implementation of the provisions in the Regulations will be phased and tied to the development and availability of appropriate technical solutions. The ICO will not take enforcement action against business and organisations that are working to address their use of cookies and/or are engaged in development work on browsers or other technical solutions. However, the ICO will take enforcement action against organisations that are not taking steps to comply with the Regulations.*”²⁰

Therefore, doing nothing does not seem a viable option for most website operators. It is highly recommended to follow legal and technical developments closely, and develop and implement solutions that could best ensure compliance with the anticipated legislation.

Organizations should consider the following steps to work towards compliance and to mitigate risks:

Audit site to identify what cookies are currently used and for what purposes

It is crucial to identify what cookies are being used and for what purposes. This will include an audit of the

¹⁸ See *supra* note 4; see also Article 29 Working Party, Working Document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU-based websites, WP 56.

¹⁹ Article 29 Working Party, Opinion 8/2010 on applicable law, WP 179.

²⁰ See *supra* note 12.

tags on your web pages that call your servers (and, if relevant, third-party servers) to drop cookies. You may be surprised to find that old tags still exist from prior tests, or from programs that no longer exist, but that are still causing cookies to be dropped. Clearly, those should be cleaned up.

For those cookies that your site intends to drop, or to allow third parties to drop, the audit will allow you to determine whether any exemptions apply. The precise scope of the exemption to Article 5(3) will largely rely on individual Member States' interpretation of the understanding of what is "strictly necessary to provide services." However, it seems safe to assume that in most cases, cookies used to deliver and improve services for users would be exempt from the general obligation to provide notice and obtain consent.

For all other cookies, in particular those used to analyze user behavior or for advertising, a two-pronged approach focused on transparency and user control should be followed. First, users should be provided with clear and transparent information about the use of cookies, and second, consent to such use should be obtained.

Focus on Improved Transparency

There are several ways to provide notice and obtain consent:

- **Review the privacy policy:** Organizations should revisit and expand their online privacy policies to ensure that full details on cookies are included. The privacy policy should include a list of the cookies used with a description of how they work, as well as the purposes for which cookies information is used, the people with whom the data will be shared, and whether the information will be combined with log-in information. The policy should also include detailed instructions on how to manage cookies. Consider adding express directions to browser settings rather than generic references. The privacy policy should be prominently placed, and be easily accessible and intelligible to users. If notice is not provided, cookies or other similar technologies should not be used.

- **Separate cookies policy:** Organizations may also consider including the explanations on cookies in a separate cookies policy that can be easily linked to, or can be shown to users when they register, or where an advertisement is placed.

- **Information outside the privacy policy:** It is advisable to provide additional notice outside the privacy policy about cookies used for analytics and advertising. For login-based systems, users can be presented with language as they register or login. For other sites, this is not an option, and operators should consider informing users about these cookies through an icon, pop-up, floater, or landing page, etc., that notifies them that their online behavior is being tracked, including how and for what purpose. Another pos-

sible option is to place text in the footer or header of the webpage which is highlighted or which turns into a scrolling piece of text when a cookie is set.

- **Inform about third-party cookies:** In addition, if cookies are dropped on behalf of third parties, or if cookies are dropped on an affinity partner's website, if at all possible, users should be notified about these cookies. Here the IAB Europe Icon Program is a good option for cookies associated with online behavioral advertising.

User Control

- **Where possible, obtain explicit (opt-in) consent:** Where possible, consider requiring users to opt-in by ticking a box. Where a user fails to tick the box, access to further services should be refused. Next to the tick box, there should be consent language and a screen showing the privacy policy. The consent language should be clear and concise and should explicitly request consent to the use of the personal data of the user visiting the website to provide services. Note that where express opt-in consent is required a tick box may not be pre-checked; consent obtained through pre-checked boxes is considered as opt-out. For third party cookies that are set or read by third parties, obtaining consent may be very difficult if not impossible. Here it will be vital that users are given more and better information about how the data might be used, and to allow users to make informed choices about what is stored on their device.

- **Provide the means for opt-out consent:** At a minimum, notices should have a means for consumers to opt-out of the setting of cookies. Opt-out language should be included in any new, enhanced notice you develop. Opt-out language in any new, enhanced notice you develop. Opt-out choices must be honored persistently, for example with a browser plug-in.

- **Work with browser companies:** Where consent may be expressed through browser settings, it is likely that the relevant national authorities will draft a list of pre-approved settings or browsers, rather than leaving it to the individual interpretation of the website operators. For now, as Microsoft (Internet Explorer), Mozilla (Firefox), and Apple (Safari) continue to roll out their versions of "Do Not Track," based on browser header approaches, carefully consider whether you are able to honor the header.

Finally, agreements with service providers should be reviewed to ensure that appropriate security standards are in place, and that purpose limitations and consent requirements are included. For example, advertising network providers may be required to obtain consent as required, through a pop-up or icon being developed by the advertising industry. To this end, organizations should be aware of the interpretation of the authorities that the icon developed by advertisers and marketers to inform the web users of the workings of cookies and behavioral tracking, while allowing users to opt-out of advertisements being shown, does not give users the chance to opt-out of being tracked.