MORRISON | FOERSTER

Legal Updates & News

Bulletins

Cookies Under the Amended ePrivacy Directive

November 2009
by Karin Retzer, Anthony Nagle

Cookies Under the Amended ePrivacy Directive

Related Practices:

- Privacy and Data Security
- Technology Transactions

After years of debate, the Council of the European Union has finally agreed on various amendments to the ePrivacy Directive (the Directive on privacy and electronic communications 2002/58/EC – "ePrivacy Directive"),[1] which include new requirements for websites that use cookies or similar tracking technologies.

These requirements have significant implications for communication and Internet service providers and the online advertising industry in general. The presidents of both the European Parliament and the European Council are due to sign the drafts into law on November 25. The 27 EU Member States will then have to implement the new requirements within 18 months of the publication date of the amendments in the EU's official journal, which is to be expected in the weeks ahead.

The introduction of the cookies and spyware requirements had gone almost unnoticed during the negotiations over the amendments because the requirements have been introduced as part of a wider EU telecommunications package. This includes an ongoing, high-profile debate about the introduction of U.S.-style breach notification requirements and the so-called "three-strikes law," which would enable local regulators to cut off individuals' Internet use if they repeatedly download illegal content. While the breach notification regime was adopted, the three-strike law was eventually rejected. These debates overshadowed the amendments agreed upon relating to cookies and other similar technologies, which were added at the last minute, meaning that online businesses only recently became aware of the amendments.

What Is the Existing Framework?

Under the existing ePrivacy Directive, it is acceptable to use cookies for legitimate purposes if the users are provided:

> *"with clear and precise information"* about the purposes of such use, *"so as to ensure that users are made aware of information being placed on the terminal equipment they are using."*

Due to the way some EU Member States such as the UK have interpreted the original cookie law when

implementing the prior version of ePrivacy Directive into local law, the business community tended to take this language to mean that it was acceptable give users the right to refuse the placement of a cookie "after" the delivery of the cookie. Under this interpretation, it was acceptable to provide the necessary information in the privacy policy on the website, and users were directed to sites which described how they could disable or reject cookies. Other Member States, such as Germany, did not adopt specific laws on the issue, but rather relied on general data protection rules.

And the New Rules?

The amendments signal a European-level shift towards prior notice and "consent."

The amended Article 5(3) refers more specifically to consent and reads as follows (redlines are against the original):

> *"Member States shall ensure that the ~~use of electronic communications networks to~~ stor**~~e~~ing of**~~information or to gain~~*oraccess to information**already** stored**~~,~~** in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned **has given his or her consent, having been** ~~is~~ provided with clear and comprehensive information**~~,~~** in accordance with Directive 95/46/EC, inter alia about the purposes of the processing**~~, and is offered the right to refuse such processing by the data controller~~**. This shall not prevent any technical storage or access for the sole purpose of carrying out ~~or facilitating~~ the transmission of a communication over an electronic communications network, or as strictly necessary in order **for the** provide**r of** ~~to provide~~ an information society service explicitly requested by the subscriber or user**to provide the service**."*

A new recital 66 is intended to add clarity relating to which the notice and consent obligations:

> *"Third parties may wish to store information on the equipment of a user, or gain access to information already stored, for a number of purposes, ranging from the legitimate (such as certain types of cookies) to those involving unwarranted intrusion into the private sphere (such as spyware or viruses). It is therefore of paramount importance that users be provided with clear and comprehensive information when engaging in any activity which could result in such storage or gaining of access. The methods of providing information and offering the right to refuse should be as user-friendly as possible. Exceptions to the obligation to provide information and offer the right to refuse should be limited to those situations where the technical storage or access is strictly necessary for the legitimate purpose of enabling the use of a specific service explicitly requested by the subscriber or user. Where it is technically possible and effective, in accordance with the relevant provisions of Directive 95/46/EC, the users consent to processing may be expressed by using the appropriate settings of a browser or other application. The enforcement of these requirements should be made more effective by way of enhanced powers granted to the relevant national authorities."*

In Member States that previously have not specifically required advance notice and consent for cookies, the practical impact of this change may be that the Member States interpret this new language to require pop-up messages (or some type of "landing" page) to ask users for their consent to use cookies before the website places a cookie on the user's computer.

The following types of cookies appear to be exempt from the requirements:

- session cookies; and
- other cookies "strictly necessary" for specific service explicitly requested by the subscriber or user.

For example, an online store receiving a specific purchase request from a user might be able to use cookies without having to obtain consent under the exception provisions (i.e. *"a specific service explicitly requested by the subscriber or user"* is excluded from the advance consent requirement).

What Type of Notice?

Recital 25 of the prior ePrivacy Directive requires that notice be provided in a format *"as user-friendly as possible."* In the past, many operators have complied with this obligation by providing notice in privacy policies and online terms of service. The amendments repeat these requirements, but it is unclear whether or not the prior practices will be sufficient. This will be resolved based on how the amendments are transposed into Member State law, and it

may be that at least some Member States adopt an "enhanced notice" mechanism, such as that advocated by the United States Federal Trade Commission:

> "a clear, concise, consumer-friendly, and prominent statement that . . . data about consumers' activities online is being collected at the site for use in providing advertising about products and services tailored to individual consumers' interests,[2]"

In the United States, this may ultimately take the form of an icon on publishers' pages (where the information is collected) or in or around the advertisements themselves, leading to a landing page with more information and a choice mechanism. This framework is likely to be incorporated into a new self regulatory program launching in the first quarter of 2010.[3]

And What Consent?

The amendments do not clarify the type of consent that will be required. Under recital 66 it may be still be possible to obtain user consent through the user's browser settings. Recital 66 expressly states that where *"technically possible and effective,"* the default browser setting or other applications are a means to provide consent. The Working Party 29 and the European Data Protection Supervisor had initially objected to this change, arguing that reference to browser settings was not technology-neutral, and it would erode the definition of "informed" consent as most users are not aware of the implications of a browser setting. However, this argument was rejected by the Council of the European Union and thus it is evident that the use of browser settings as a means to achieve consent is consistent with the amendments. There is also a strong argument that the language on browser settings in recital 66 indicates that opt-out or implicit consent is sufficient because a default browser setting cannot be viewed as explicit or opt-in consent for a specific website. Rather, the default setting will constitute implicit or opt-out consent.

Moreover, the language in the amendments relating to cookies is not the same as the language used when opt-in consent was specifically wished for commercial communications. For example, in the section relating to "spam" the obligation is to obtain "prior explicit" consent or opt-in consent. That language is not used in the cookies section. Thus there is a good argument that the consent need not be opt-in. In the end, it will be for each Member State to transpose these obligations and to determine the type of consent allowed. Notwithstanding these arguments, we anticipate that at least some Member States will make a strong push to incorporate an opt-in standard under the amendments.

Who and What Is Covered?

Strictly speaking, the ePrivacy Directive only applies to the processing of personal data in connection with the provision of publicly available electronic communication services in public communications networks within the EU, including public communications networks which support data collection and identification devices. The proposal to expand its scope to cover website operators and corporate networks or closed user groups was rejected (recital 55). There may be an argument that only telecommunication and Internet service providers are covered. That said, the cookies amendments target users, and we anticipate that most Member States will implement the rules to cover websites broadly.

As for the types of technologies covered, the provisions aim at cookies – small text files which are sent by a website to a user's web browser and collect information about the user's web use (which is later collected by the website). The new rules appear to apply to other applications as well, such as web beacons, ad tags, JavaScript code, or other technologies that are integral to the functioning of the Internet or used for advertising, provided they are used to store or access information on a user's computer or other device.

What Is Next?

Due to the relatively short implementation period of 18 months, Member States must now begin interpreting and implementing the amended ePrivacy Directive by enacting local laws in each EU Member State. Legislators in Member States are expected to run a consultation process prior to amending the local laws. This will give local industry and businesses the opportunity to lobby and present any issues and concerns about the new requirements. Industry will likely emphasize the threat to the workings of the Internet if all such features are made subject to onerous opt-in requirements. Given the unclear language of the Directive, there is certainly room for local variation.

In any event, the amendments may well mean that existing requirements are enforced more actively.

The amended ePrivacy Directive provides for a new Article 15a:

> *"Member States shall lay down the rules on penalties, including criminal sanctionswhere appropriate, applicable to infringements of the national provisions adoptedpursuant to this Directive and shall take all measures necessary to ensure that theyare implemented. The penalties provided for must be effective, proportionate anddissuasive and may be applied to cover the period of any breach, even where thebreach has subsequently been rectified."*

Therefore, the real impact of the new cookie requirements may be in the area of enforcement rather than any new substantive requirements. Under the original ePrivacy Directive, Member States did not go to any great lengths to enforce the cookie laws. Whether the amendments under the revised ePrivacy Directive will bring greater enforcement is not clear at this stage, but the EU regulators have been provided with increased enforcement powers, and there are now greater penalties.

Footnotes

[1] Available in English here.

[2] See*FTC Staff Report: Self-Regulatory Principles For Online Behavioral Advertising* (February 12, 2009), available at http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

[3] See *Self-Regulatory Principles for Online Behavioral Advertising* (American Association of Advertising Agencies, Association of National Advertisers, Council of Better Business Bureaus, Direct Marketing Association, and Interactive Advertising Bureau) (July 2, 2009), available at http://www.the-dma.org/government/ven-principles%2007-01-09%20FINAL.pdf.
