CLIFFORD
CHANCE

Global Technology Group
Alerter - May 2011

Deadline for compliance with new rules on online privacy matters approaches

New Directive on user privacy rights and data protection

By 25 May 2011, the EU Member States must implement the new European e-Privacy Directive, which was adopted on 25 November 2009. The e-Privacy Directive amends various earlier Directives, introducing measures aimed at improving data and privacy protection of users and subscribers of communications network services. The new Directive introduces, *inter alia*, measures that:

- Require explicit user consent for storage of cookies;
- Mandate information on security and integrity incidents; and
- Impose certain information obligations on on-line service providers.

Although Member States and market participants face an imminent deadline for implementation of and compliance with the new e-Privacy Directive, no meaningful guidance in that regard has yet been provided by relevant EU or national authorities. This leaves service providers with the task of unilaterally assessing how to comply with measures imposed upon them by the e-Privacy Directive. This Alerter compiles some relevant guidance offered by industry bodies. Close monitoring of the current debates on implementation of and practical compliance with the e-Privacy Directive is however advisable.

I. Cookies

Many web services depend on cookies to function properly. Article 2 of the e-Privacy Directive imposes stricter obligations on service providers in respect of the local storage of cookies, according to which:

"(…) the storing of information, or the gaining of access to information already stored in the terminal equipment (e.g. a computer system) of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information (…) "

Thus, service providers will now be required to obtain consent before storing any data locally on a computer system of a user or accessing data already stored locally. It is no longer sufficient for service providers to inform the user (*e.g.,* through a data protection statement) about the type of data that is processed. The Directive does not specify, however, how this consent should be obtained.

In the absence of any guidance from the European Commission in this regard, a preliminary interpretation of Article 2 may imply that service providers will be required to implement some mechanism or technical solution to request and collect the users' consent to the storage of data in cookies before granting access to any website or related services that use cookies, and, in case of a refusal, they will have no alternative but to deny access to their services altogether.

If you would like to know more about the subjects covered in this publication or our services, please contact:

Thomas Vinje +32 2 533 5929

Joachim Fleury +44 20 7006 8050

Bernd Meyer-Witting +49 69 71993115

Jan Wittrodt +49 69 7199 1248

Richard Jones +44 207006 8238

To email one of the above, please use firstname.lastname@cliffordchance.com

Clifford Chance, Avenue Louise 65, Box 2, 1050 Brussels, Belgium
www.cliffordchance.com

This view is supported by the opinion of the Article 29 Working Party, according to which (i) consent must be obtained before the cookie is placed or information stored in the user's terminal equipment is collected (prior consent) and (ii) prior information about the sending and purposes of the cookie must be provided to the user (informed consent).[1]

However, the preamble of the e-Privacy Directive provides that (i) the users' consent to processing may be expressed by using the appropriate settings of a browser or other application and (ii) the methods of providing information and offering the right to refuse should be as user-friendly as possible.

This has led the UK Information Commissioner (**"ICO"**) initially to suggest that Article 2 may only require the implementation of technical measures to prevent unnoticed and unsolicited storage of cookie data. Thus, a setting of the web browser to accept cookies, even by default, would be considered to constitute consent to the collection of data following the argument that any other solution would be impracticable.

Others consider this to be too liberal an interpretation, doubting whether it is in compliance with the strict wording of Article 2 - in particular given the general requirement, established in the framework Data Protection Directive (95/46/EC), that consent must be specific and freely given. For example, the Article 29 Working Party has opined that data subjects cannot be deemed to have consented simply because they use a browser or other application which by default enables the collection and processing of their information. Thus, according to the Article 29 Working Party, authorization for cookie processing cannot be deduced from a user having failed to take certain precautions in his browser settings.

Another practical issue is the question of how service providers ought to keep track of users who have consented to the storage of data and the use of cookies. Although such information could also be stored in cookies, this would appear to collide with technical solutions of modern web browsers such as Firefox, which offer automatically to delete cookies at the end of each browsing session. As a consequence, users would have to consent to the storage of data and use of cookies each time they visit a website or request a service. Other solutions would require the service provider permanently to store information as to whether a user has consented to the use of cookies in an independent database. This solution, however, would require the service provider to identify the user, as otherwise the service provider would not be able to determine whether the relevant user has already given his or her consent. This would appear to contradict the overall aim of the e-Privacy Directive.

The Commission has yet to offer any guidance on the practical application of the e-Privacy Directive and compliance with Article 2.

In the meantime, EU Member States are in the process of implementing or - as in the UK[2] - already have implemented the e-Privacy Directive, albeit similarly without having provided meaningful guidance on the above issues. Whilst the German government has introduced a draft bill dated 4 March 2011[3] transposing the e-Privacy Directive into German law, it has avoided taking a clear position on the cookie issue mentioned above and only provides that the implementation of various issues of the Directive (including cookies) are the subject of some debate at a European level, and that the outcome of such debate will determine the legislative procedure.

Similarly, the UK government recently expressed the view that it has "no idea" what is required for compliance with the new rules on cookies in the e-Privacy Directive.[4] However, the UK government announced that enforcement action would not be taken "in the short term."

At present, only the UK ICO has published guidance on the practical implementation of the e-Privacy Directive. According to this guidance, service providers should

- Check what type of cookies and similar technologies they use;
- Assess how intrusive their use of cookies is; and
- Decide what solution to obtain consent will be best suited in their circumstances.

Short of providing prescriptive guidance with respect to a practical solution, the ICO proposes to gain consent through the use of (i) pop-ups, (ii) terms and conditions or (iii) by placing some text in the footer or header of the web page which is highlighted when a service provider wants to set a cookie.

[1] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf
[2] http://www.legislation.gov.uk/uksi/2011/1208/pdfs/uksi_20111208_en.pdf
[3] http://www.bundesrat.de/cln_179/nn_8336/SharedDocs/Drucksachen/2011/0101-200/129-11,templateId=raw,property=publicationFile.pdf/129-11.pdf.
[4] http://www.ico.gov.uk/~/media/documents/library/Privacy_and_electronic/Practical_application/advice_on_the_new_cookies_regulations.pdf

As regards (ii) and (iii), these measures would only work where the user either signs up for a specific service or where a cookie is set during the browsing session but not at the very beginning of such a session. Many cookies are, however, set at the beginning of a browsing session. Accordingly, the majority of service providers would be limited to option (i), forcing the service provider to present the user with a pop-up before they could visit the site. Overall, the ICO guide does not present any new ideas as to how to comply with the measures and provisions of the e-Privacy Directive.

Moreover, and contrary to its early statement, the ICO has stated that service providers cannot rely on browser settings to assume that users have given their consent for cookies to be stored, thus rejecting a solution that is already widely used.

Third-party cookies

Every website which uses advertisements inevitably stores so-called third party cookies. These third party cookies are one of the major concerns of service providers, which subsidize their web content through advertisements. The Internet Advisory Bureau (**"iab"**), a European trade association, recently introduced a self-regulatory framework[5] with a view to providing a practical solution for online behavioral advertising (including third party cookies) which aims at complying with the e-Privacy Directive. This framework envisages the introduction of a uniform pictogram (icon) across all European countries. A click on this icon would display information about some or all of the companies involved in providing the advert and would also allow users to visit a website where they could turn off online behavioral advertising, including the placement of third party cookies for the respective advertisement network. According to the Director of Regulatory Affairs of the iab, Nick Stringer, the UK government has accepted this self-regulatory framework as being in compliance with the e-Privacy Directive. Service providers could adopt the framework by signing the framework principles and according to the iab, 50 companies across Europe have already done so. It is unclear at present whether other national governments will follow this approach and accept that this self-regulatory framework complies with the e-Privacy Directive.

II. Information on security and integrity incidents

While many US States have since 2002 enacted security breach notification laws, which require companies to immediately disclose a breach of data to customers, there is currently no general security breach notification regime available in the EU, *i.e.* which would universally apply to all market participants which are processing personal data.

Pursuant to Article 2 of the e-Privacy Directive, however, service providers will now be obliged to inform relevant authorities and users about security and integrity incidents which affect or may have affected personal data without undue delay.

An exception may apply where the provider has demonstrated to the satisfaction of the relevant authority that it has implemented appropriate technological protection measures and that those measures were applied to the data affected by the security breach.

III. Information obligations

The e-Privacy Directive will require service providers to provide additional information to their users and subscribers before concluding a contract. The information to be provided includes:

- Whether access to emergency services and caller location information is being provided;
- Minimum service quality levels;
- Information on procedures to measure the shaping of traffic;
- The types of maintenance service offered and customer support services provided;
- Details of prices and tariffs, payment methods and any differences in costs due to payment methods;
- The duration of the contract and the conditions for renewal and termination of services and of the contract; and
- The type of action that might be taken to deal with security or integrity incidents or threats and vulnerabilities.

[5] http://www.iabeurope.eu/media/51925/iab%20europe%20oba%20framework_merged%20ii.pdf

Whilst service providers are already to a large extent required to provide some or even all of the above information pursuant to the different national laws of the EU Member States, the e-Privacy Directive aims at harmonizing these national laws at a European level.

Summary

A number of aspects of the practical implementation of the e-Privacy Directive remain unclear and unresolved in the current state of implementation, in particular as regards the use of cookies. It remains to be seen whether the Commission, national governments or relevant data protection authorities will provide service providers with sufficient guidance as to compliance with the measures and provisions contained in the e-Privacy Directive.

Meanwhile, service providers should closely monitor the ongoing discussion(s) at European and national levels in order to be able to adapt their relevant services to the developments and outcome of such discussions in time before national adoptions of the e-Privacy Directive enter into force.