Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

European national news

Nick Pantlin *

Herbert Smith Freehills LLP, London, United Kingdom

Keywords:
Internet
ISP/Internet service provider
Software
Data protection
IT/Information
Technology
Communications
European law/Europe

ABSTRACT

This article tracks developments at the national level in key European countries in the area of IT and communications and provides a concise alerting service of important national developments in key European countries. It is co-ordinated by Herbert Smith Freehills LLP and contributed to by firms across Europe. Part of its purpose is to complement the Journal's feature articles and briefing notes by keeping readers abreast of what is currently happening "on the ground" at a national level in implementing EU level legislation and international conventions and treaties. Where an item of European National News is of particular significance, CLSR may also cover it in more detail in the current or a subsequent edition.

1. Belgium

Cédric Lindenmann, *Associate,* cedric.lindenmann@stibbe.com *and* **Carol Evrard**, *Associate,* carol.evrard@stibbe.com *from Stibbe, Brussels (Tel.: +32 2533 53 51).*

No contribution for this issue

2. Denmark

Arly Carlquist, *Partner,* ac@bechbruun.com *and* **Niclas Jensen**, *Junior Associate,* nic@bechbruun.com *from Bech-Bruun, Copenhagen office, Denmark (Tel.: +45 7227 0000).*

2.1. *The Danish Act on Network and Information Security*

On 1 July 2016 the Danish Act on Network and Information Security came into force. The new act results in stricter requirements for the telecommunications providers' network and information security and emergency preparedness. Consequently telecommunications providers must, to a greater extent, take society's dependence on the telecommunication networks into account and ensure that electronic communication can take place in emergencies and other extraordinary situations.

The Centre for Cyber Security ("**CFCS**"), a part of The Danish Defence Intelligence Service, is the national authority of IT security in Denmark.

The law authorises CFCS to lay down rules regarding minimum requirements with respect to information security for providers of publicly available networks and services. Furthermore, the law authorises CFCS to issue specific instructions to providers of publicly available networks and services, and to impose punitive sanctions if the issued instructions are not followed.

CFCS has already introduced several new concepts. One noteworthy concept is "essential commercial service providers" who are subject to more rigorous rules than ordinary commercial service providers. CFCS has also introduced the concept "critical network components, systems and tools", which results in a duty for an essential commercial service provider to notify CFCS prior to entering into negotiations with a supplier, and on top of that a potential 10 working day standstill period.

For further information see: www.herbertsmithfreehills.com.

* *Corresponding author.* Herbert Smith Freehills, Exchange House, Primrose St, London EC2A 2HS.
E-mail address: nick.pantlin@hsf.com.

http://dx.doi.org/10.1016/j.clsr.2016.12.002

From 1 January 2017 a service provider is obliged to ensure that its employees and representatives are security cleared, if the persons in question have access to interception equipment or systems concerning the secrecy of correspondence.

3. France

Alexandra Neri, *Partner,* alexandra.neri@hsf.com *and* **Jean-Baptiste Thomas-Sertillanges**, *Avocat,* Jean-Baptiste.Thomas-Sertillanges@hsf.com *from the Paris Office of Herbert Smith Freehills LLP (Tel.: +33 1 53 57 78 57).*

No contribution for this issue

4. Germany

Dr. Alexander Molle, *LL.M. (Cambridge), Counsel,* alexander.molle@gleisslutz.com*, from the Berlin Office of Gleiss Lutz, Germany (Tel.: +49 30800979210).*

4.1. *Dynamic IP addresses as personal data*

The ECJ recently decided that dynamic IP addresses might constitute personal data under the Data Protection Directive (95/46/EC). This decision has far-reaching consequences for online media service providers.

In the case under review, the claimant visited several public websites operated by German Federal institutions which, in some cases, stored access data including dynamic IP addresses. The claimant filed for an order restraining the website provider from storing the dynamic IP addresses except for cases where storage of the IP addresses is necessary for the operation of the website.

The ECJ had to decide whether dynamic IP addresses are personal data according to Article 2 of the Directive, even though the website provider was not able to identify the user without additional information from the respective Internet service provider. The ECJ argued that insofar as the identification of the person concerned is possible by combining the dynamic IP address with the data held by the Internet service provider and legal means exist to get hold of such data from the Internet service provider, the person is identifiable. Thus, *de facto* dynamic IP addresses constitute personal data in Germany as a website provider has – e.g. in an infringement situation – legal means to get access to the users' data stored by the Internet service provider.

The ECJ further decided that the narrow interpretation of a certain provision in the German Telemedia Act according to which collection of personal data without user's consent shall only be allowed if and to the extent such data collection is necessary for the consummation of the concrete service in question or for billing purposes does not take the general operability of the service as a legitimate interest of the provider sufficiently into account and is, therefore, too narrow and not compliant with the Directive. The ECJ noted that the Directive sets out an exhaustive list of cases in which the processing of personal data can be regarded as being lawful without users' consent. Member States cannot broaden or limit this scope.

In any case, storing of personal data e.g. for marketing purposes without user's consent is neither allowed under the Directive nor the German Telemedia Act. The consequence of this is that storing dynamic IP addresses by online media service providers for such purposes without users' consent can infringe data protection law.

5. Italy

Salvatore Orlando, *Partner,* s.orlando@macchi-gangemi.com; **Laura Liberati**, *Senior Associate*, l.liberati@macchi-gangemi.com; **Arnaldo Salvatore**, *Partner*, a.salvatore@macchi-gangemi.com, *Rome office of Macchi di Cellere Gangemi (Rome office tel. +39 06 362141).*

No contribution for this issue

6. The Netherlands

Barbra Bulsing, barbra.bulsing@stibbe.com@stibbe.com*, Amsterdam office of Stibbe (Tel.: +31 20 546 0332).*

No contribution for this issue

7. Norway

Dr. Rolf Riisnæs, *Partner,* rri@wr.no, **Dr. Emily M. Weitzenboeck**, *Senior Associate*, emw@wr.no, *Wikborg Rein Advokatfirma AS (as from 1.1.2017), Norway (Tel. +47 22 82 75 00).*

7.1. *Consumer ombudsman critical of the proposed liberalisation of advertising in audio-visual media services*

The European Commission's proposal for an amendment to the Audiovisual Media Services Directive (2010/13/EU) published in May 2016 was sent for public consultation by the Norwegian Ministry of Culture. In its response during the consultation process, the Consumer Ombudsman was critical of the proposed changes to the provisions on sponsorship and product placement, as well as to the rules on the frequency of television advertising spots and teleshopping spots.

The proposal would remove the prohibition of "special promotional references" in audio-visual media services or programmes that are sponsored, as well as in product placement. The Consumer Ombudsman warned against a trend which increasingly challenges and undermines the fundamental "principle of separation" whereby a distinction must be maintained between commercial messages and editorial content. The Ombudsman stated that product placement which, by definition, is subtle and mixed together with non-commercial content, raises questions to the fundamental rule that marketing must be clearly identified as marketing.

The proposal does not provide how consumers can identify product placement. One possibility, suggested by the Consumer Ombudsman, would be to consider laying down a rule that a neutral statement that there is product placement, as is the practice today, must be visible at the point in time when the product is shown during the programme.