COMPUTER LAW & SECURITY REVIEW 31 (2015) 705–709

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

The regular article tracking developments at the national level in key European countries in the area of IT and communications – co-ordinated by Herbert Smith Freehills LLP and contributed to by firms across Europe. This column provides a concise alerting service of important national developments in key European countries. 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).*

1.1. *Belgian Privacy Commission issues recommendation concerning Facebook*

On 13 May 2015, the Belgian Privacy Commission (the "**BPC**") published a recommendation relating to the law applicable to users and providers of Facebook services, dealing in particular with plug-ins and cookies. This recommendation has been adopted in response to Facebook's modified terms of use which were introduced on 30 January 2015.

The BPC contests Facebook's assertion that Facebook Ireland should be considered as the data controller for the processing of European users' data. According to the BPC, the real decision maker is Facebook Inc., which is established in the United States. Facebook Ireland would not be able to determine the means and purposes of the processing of Belgian user data. Therefore, the BPC considers Facebook Inc., and not Facebook Ireland, to be the data controller for such processing.

Furthermore, the BPC argues that although Facebook Belgium SPRL only conducts advertising and lobbying activities, those activities are inextricably connected to the activities of Facebook Inc. Therefore, according to the recent decision of the European Court of Justice in the *Google Spain* case (C-131/12), the Belgian Data Protection Act (the "**BDPA**") must apply.

The fact that Facebook Belgium SPRL does not process any personal data itself has no impact on this finding. According to the *Google Spain* case, "a Member State's national data protection law is applicable if the activities of an establishment, incorporated in that Member State, are inextricably connected to the activities of the controller, regardless of whether the establishment performs data processing activities or not."

For the sake of completeness, the BPC also referred to the application of Article 4 § 1(c) of the BDPA. According to this provision, the BDPA applies in this situation because Facebook Inc., as the data controller, is established outside of Europe and makes use of automated means situated in the territory of a Member State (i.e. cookies).

* Herbert Smith Freehills Exchange House, Primrose St, London EC2A 2EG, United Kingdom. Tel.: +44 20 7374 8000.
E-mail address: Nick.Pantlin@hsf.com.

http://dx.doi.org/10.1016/j.clsr.2015.07.008
0267-3649/

The second part of the recommendation addresses the question of Facebook's use of social plug-ins. By using social plug-ins Facebook is allegedly gathering information on internet users' surfing behaviour (whether using Facebook or not) on different websites without having obtained such users' consent. Therefore, Facebook is allegedly processing personal data without any legal basis to do so.

Meanwhile, the BPC has initiated legal proceedings against Facebook. It is interesting to see that the BPC has decided to launch a civil lawsuit instead of reporting a violation of the BDPA to the public prosecutor, as would usually be the case. The President of the Court of First Instance in Brussels has scheduled a court hearing for 21 September 2015. Meanwhile, the BPC is claiming periodic penalty payments of 250,000 EUR per day for continued non-compliance by Facebook with the BDPA.

2. Denmark

Arly Carlquist, *Partner,* ac@bechbruun.com *and* **Henrik Syskind Pedersen**, *Attorney,* hsp@bechbruun.com *from the Copenhagen Office of Bech-Bruun, Denmark (Tel.: +45 7227 0000).*

2.1. *Healthcare related smartphone apps may pose security risks*

Today, a smartphone app is available for almost any purpose you can imagine, including various healthcare related smartphone apps which have been introduced and are available whether directly to consumers for their own use or to healthcare professionals.

These apps that may be used in healthcare include those introduced for professional use to calculate the dose of a medicine, to allow for a diagnosis of skin cancer based on an image or to work as a stethoscope for physicians. On the other hand, there are smartphone apps for consumers which may be used to measure blood pressure or blood sugar.

These smartphone apps must be developed, designed and marketed in accordance with applicable law. The legal framework in place provides that smartphone apps must satisfy the same regulatory requirements as applicable to other goods and services provided within the healthcare sector.

However, a recent Danish study on healthcare related smartphone apps has attracted attention from Danish media and the Danish Healthcare and Medicine Authority. The study showed that not all available healthcare related smartphone apps comply with the applicable CE marking requirements.

Smartphone apps qualify as medical devices and are therefore subject to the Medical Device Directives in order to be legally admitted to the EU market. This includes the requirement concerning CE marking. The purpose of these requirements is the elimination of security risks in the healthcare sector.

Thus, the study indicates a need for an increased focus on regulatory compliance in terms of healthcare related smartphone apps. Developers and publishers of healthcare related smartphone apps must ensure compliance with regulatory requirements not only with respect to CE marking but also in regard to all regulatory requirements, including marketing legislation, handling of personal data, etc.

3. France

No contribution for this issue.

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).*

4. Germany

Dr. Stefan Weidert, *LL.M. (Cornell), Partner (*stefan.weidert@gleisslutz.com*) and* **Dr. Martin Hossenfelder,** *Associate (*martin.hossenfelder@gleisslutz.com*), from the Berlin Office of Gleiss Lutz (tel.: +49 30 800 979 0).*

4.1. *Lawfulness of framing*

In July 2015, the German Federal Court of Justice (**BGH**) ruled on "framing", which is generally defined as the combination of two separate websites within the same website that divides the screen into multiple non-overlapping windows.

In the case at hand, the plaintiff, a company in the business of water filtration systems, had produced a short video on water contamination which was uploaded to YouTube, although it was not clear whether that was done with or without the plaintiff's consent. The defendants, two commercial agents of a competitor of the plaintiff, then embedded the video on their websites for marketing purposes, so that upon clicking on the link the video was played via a YouTube server while remaining embedded in the defendants' websites.

The plaintiff argued that the defendants had made the video available to the public within the meaning of the German Copyright Act ("**UrhG**") without its permission. The Federal Court of Justice took a different position (following the decision of the ECJ on 21 October 2014 – C-348/13 regarding Art. 3(1) of Directive 2001/29/EC), ruling that the mere combination of content contained on a third party webpage with own content by way of framing would not per se constitute a copyright violation. It argued that only the original content owner (in this case the plaintiff) could decide on whether the content would remain publicly available or not. However, the court also emphasised that framing is allowed only if the initial publication had occurred with the copyright owner's consent, which was a matter of dispute between the parties. Therefore, the court referred the case back to the lower court.

5. Italy

Salvatore Orlando, *Partner,* s.orlando@macchi-gangemi.com *and* **Stefano Bartoli**, *Associate,* s.bartoli@macchi-gangemi.com *from the Rome office of Macchi di Cellere Gangemi (Tel.: +39 06 362141).*