Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

EU update☆

Scott Allardyce, Chris Boyle, Emma Charlton, Patricia Collis, Claire Davies, Lottie Fry, Naomi Hazenberg, Louisa Jacobs, Tom Ohta, Christopher Smits, Mark Watts, Faye Weedon, Osman Zafar*

Bristows LLP, United Kingdom

Keywords:
EU law
Intellectual property
Information technology law
Telecommunications law

ABSTRACT

This is the latest edition of the Bristows column on developments in EU law relating to IP, IT and telecommunications. This news article summarises recent developments that are considered important for practitioners, students and academics in a wide range of information technology, e-commerce, telecommunications and intellectual property areas. It cannot be exhaustive but intends to address the important points. This is a hard copy reference guide, but links to outside web sites are included where possible. No responsibility is assumed for the accuracy of information contained in these links.

1. Data protection/privacy

1.1. *European Commission calls for more robust Safe Harbour Framework*

In the wake of revelations surrounding the large-scale collection of personal data by US intelligence agencies, the Commission has released a communication calling for the strengthening of the Safe Harbour scheme. The Commission also called for the expedient adoption of EU data protection reforms and an extension to the US administration's commitments to protect and safeguard the personal data of EU residents.

The communication stressed the importance of trans-Atlantic data flow for commercial and law enforcement purposes. However, it also highlighted the fact that large-scale US data collection programmes such as PRISM had negatively affected trust between the EU–US partnership.

The Commission stated that both the EU and the US needed to take action to improve data security and rebuild trust and it called for the adoption of the EU data protection reforms by Spring 2014. The proposed reforms would require, among other things, non-EU companies to apply EU data protection laws when they offer goods and services to EU customers.

The Commission called for a complete 'stock-take' of the Safe Harbour scheme after identifying weaknesses such as non-compliance by some self-certified US companies. The Commission also questioned the use of the 'national security exception' by the US administration and re-emphasised that this exception is only to be used to the extent it is strictly necessary and proportionate.

The Commission also sought commitments from the US that personal data held by private entities in the EU will not be directly accessed by US law enforcement agencies, rather, this data will only be accessed through formal channels of co-operation (such as the Passenger Name Records, and the Terrorist Finance Tracking Program ("TFTP")) under very strict controls. The communication identified that a joint review of the implementation of these mechanisms did not identify any breaches by the US authorities. However, the EU and US have agreed to advance the next joint review of the TFTP agreement to Spring 2014.

☆ **Mark Watts** (Mark.Watts@bristows.com) Partner, Bristows LLP and member of the CLSR Professional Board (Tel.: +44 (0)20 7400 8000). For further information about Bristows LLP see: www.bristows.com.

* *Corresponding author.*

0267-3649/$ – see front matter © 2014 Bristows. Published by Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.clsr.2014.02.002

The Commission was optimistic that the current negotiations of an "umbrella agreement" for the exchange of police and judicial data would result in a high level of security for EU and US citizens, but stressed the agreement must come with appropriate procedural safeguards.

Finally, the Commission called for constructive engagement from both sides of the Atlantic to overcome the current tensions and to rebuild trust in EU–US data flows. The Commission also noted that the on-going data protection reforms provided the EU and US with the unique opportunity to set the standard internationally.

A copy of the communication is available here: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0846:FIN:EN:PDF.

1.2. *CJEU rules public authority subject access fees are lawful*

The CJEU has ruled that Article 12(a) of Directive 95/46/EC must be interpreted as not to preclude the levying of fees in respect of the communication of personal data by a public authority, but the level of these fees must not exceed the cost of communicating such data (Case C-486/12).

Article 12(a) grants data subjects the right to access information held by a data controller including confirmation of whether their data is being processed and the purpose for the processing. This data must be communicated to the data subject in an intelligible form "without constraint at reasonable intervals and without excessive delay or expense".

The CJEU referral arose in the Netherlands where national law enables individuals to obtain a transcript (certified if required) of their personal data that are being processed by local authorities. The national law allows duties to be levied on the services provided by local authorities at a rate that does not exceed the estimated expenditure.

In the referring case, X requested access to her personal data from a local authority and she was duly provided with a certified transcript of her data and charged 12.80 Euro. X stated that she did not request the data in the form of a certified transcript and disputed the fee. The national court referred the issue of whether a fee could be levied for the transcript and whether the fee was excessive.

The CJEU clarified that the wording "without excessive delay or expense" within Article 12(a) 95/46/EC meant without excessive delay or excessive expense. Therefore, the Article does not preclude a public authority from levying a fee so long as it does not exceed the cost of communicating the data. The CJEU stated that it was for the national court to carry out any verifications of the costs as necessary, having regard to the circumstances of the case.

The judgment can be found at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=145533&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=357216.

1.3. *Advocate General finds Data Retention Directive incompatible with right to privacy*

Advocate General (AG) Cruz Villalón has given the Opinion that the Data Retention Directive (2006/24/EC) is incompatible with Article 52(1) of the Charter of Fundamental Rights in relation to the regulation, access and use of personal data.

Article 51(2) of the Charter states that any limitation to the exercise of a fundamental right must be provided for by law and it must be proportionate. The AG found that "*[t]he Directive constitutes a serious interference with the right of citizens to privacy, by laying down an obligation on the providers of telephone or electronic communication services to collect and retain traffic and location data for such services.*"

The AG found that the Directive's objective of ensuring that such data are available for the purpose of investigation and prosecution of serious crime is proportionate. However, the Directive is non-compliant in two respects.

First, the Directive fails to set out the principles governing access and use of data by public authorities and limitations on how long they can retain the data. Therefore, the Directive does not comply with the requirement of the Charter that an interference with a fundamental right must be provided for by law. Second, the requirement of member states to ensure data are kept for two years is disproportionate. The AG sees no justification for setting the period above one year.

The AG has stated that the effects of the invalidity finding should be suspended until the EU legislature has adopted the necessary measures required to remedy the invalidity, so long as such measures are adopted within a reasonable period.

The AG's Opinion can be found here: http://curia.europa.eu/juris/document/document.jsf?text=&docid=145562&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=237428.

1.4. *Advocate General gives opinion that legal analysis of individual's situation is not personal data*

Advocate General (AG) Sharpston has concluded that the legal analysis of an individual's situation does not constitute their personal data. The case considers three individuals claiming entitlement of access to an internal document ('the minute') containing legal analysis on whether to grant their residency in the Netherlands.

The Opinion has sparked interest because of the interplay between Article 12 of the Data Protection Directive, which sets out the right of data subject access to personal data, and Article 8(2) of the Charter of Fundamental Rights, setting out the manner in which access to personal data may be provided.

In her Opinion, the AG takes a broad approach to personal data. Nevertheless, she concludes that, "*only information relating to facts about an individual can be personal data. Except for the fact that it exists, a legal analysis is not such a fact. Thus, for example, a person's address is personal data but an analysis of his domicile for legal purposes is not.*" As such, legal analysis itself is not information relating to an identifiable person. The AG further concludes that legal analysis is not a form of processing, and even if it were it is neither automatic nor in a manual filing system and therefore still not covered by the Directive.

However, if the CJEU finds that legal analysis does amount to personal data, the AG confirms that access to it should be granted under Article 12 of the Directive. It does not however confer a blanket right of access to any specific document containing personal data. Therefore, an individual would not