HUNTON& WILLIAMS

EUROPEAN PRIVACY & E-COMMERCE ALERT

April 2008

Contacts

Brussels Office
Park Atrium
Rue des Colonies 11
1000 Brussels
Belgium
P: +32 (0)2 643 58 00
F: +32 (0)2 643 58 22

Christopher Kuner
+32 (0)2 643 58 56
ckuner@hunton.com

Dr. Jörg Hladjk
+32 (0)2 643 58 28
jhladjk@hunton.com

Isabelle Chatelier
+32 (0)2 643 58 33
ichatelier@hunton.com

Cedric Burton
+32 (0)2 643 58 29
cburton@hunton.com

London Office
30 St Mary Axe
London EC3A 8EP
+44 (0)20 7220 5700 Phone
+44 (0)20 7220 5772 Fax

Bridget C. Treacy
+44 (0)20 7220 5731
btreacy@hunton.com

EU: ECJ Renders Judgment in Promusicae Case

On January 29, 2008, the European Court of Justice (ECJ) rendered its judgment in Promusicae, the first case in which the Court has specifically dealt with the tension between data protection and online enforcement—see Case C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU*.

In its judgment, the Court found that EU Member States are not obliged under Community law to require disclosure of personal data in the context of civil proceedings for the purpose of copyright protection, but that they may require such disclosure, and that in transposing the various directives on intellectual property, e-commerce and data protection, Member States must strike a fair balance between the fundamental rights that they protect, and must respect general principles of Community law, such as the principle of proportionality. This case was initiated by the Spanish rightsholder group Promusicae, which sought to obtain a court order in Spain against the internet service provider (ISP) Telefónica obliging the latter to disclose identity data on P2P users of the KaZaA network. Such users were engaged in the illegal uploading of copyrighted musical works. Telefónica argued that the communication of such data was authorized under Spanish law only for a criminal investigation or to safeguard public security and the national defense. The Spanish court initially granted the order sought by Promusicae, but following an appeal by Telefónica decided to stay the proceedings and consult the ECJ on the conformity of Spanish law with Community law.

The ECJ judgment is available (in English) at: http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=en&newform=newform&alljur=alljur&jurcdj=jurcdj&jurtpi=jurtpi&jurtfp=jurtfp&alldocrec=alldocrec&docj=docj&docor=docor&docop=docop&docav=docav&docsom=docsom&docinf=docinf&alldocnorec=alldocnorec&docnoj=docnoj&docnoor=docnoor&typeord=ALLTYP&allcommjo=allcommjo&affint=affint&affclose=affclose&numaff=C-275%2F06&ddatefs=&mdatefs=&ydatefs=&ddatefe=&mdatefe=&ydatefe=&nomusuel=&domaine=&mots=&resmax=100&Submit=Submit

The ECJ press release is available (in English) at: http://curia.europa.eu/en/actu/communiques/cp08/aff/cp080005en.pdf

EU Commission Brings Suit against Germany

On November 22, 2007, the European Commission brought before the European Court of Justice (ECJ) an action against the Federal Republic of Germany for failure to fulfill its obligations under the second sentence of Article 28(1) of Directive 95/46/EC (Case C-518/07), which requires national data protection authorities (DPAs) to be independent. The

European Commission considers that the Federal Republic of Germany has not fulfilled these obligations, since the supervisory authorities responsible for the monitoring of data processing within the private sector in the German *Länder* are subject to State supervision and thereby do not fulfill the requirement of "complete independence".

Background information about Case C-518/17 is available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:037:0008:0009:EN:PDF

EU Commission Launches Public Consultation on RFID Recommendation

The European Commission is currently drafting a recommendation that will address some of the privacy concerns expressed by stakeholders during a first public consultation on Radio Frequency Identification (RFID) held in 2006. The Commission is now conducting a broad consultation open to all interested parties on the articles that it considers including in its recommendation on the implementation of privacy, data protection and information security principles in applications supported by RFID. The recommendation is scheduled to be adopted before the summer of 2008. The consultation will end on April 25, 2008, after which the various contributions will be published on the Commission's web site, unless otherwise requested.

Further information on the consultation is available at: http://ec.europa.eu/yourvoice/ipm/forms/dispatch?form=RFIDRec

Finland Requires Opt-in Consent for "Tell-a-Friend" Marketing

New guidelines jointly published on January 15, 2008 by the Data Protection Ombudsman, the Consumer Agency and the Consumer Ombudsman introduce an opt-in regime for "tell-a-friend" marketing (so-called "viral" marketing) involving text messages and electronic mails. Pursuant to the Finnish Act on the Protection of Privacy in Electronic Communications, electronic commercial communications may not be sent without the recipient's prior and explicit consent. The guidelines clarify that the Act is also applicable to situations where such communications are exchanged between private individuals. Prior consent of the recipient is thus required when users forward a message originally prepared by a company to their private social contacts. The DPA's guidance is available (in Finnish and Swedish) at: http://www.tietosuoja.fi/42171.htm

France: CNIL Releases New Biometric Policy Guidelines

On December 12, 2007, the French Data Protection Authority (CNIL) presented new guidance on the conditions that must be met in order to use biometric-based identification systems. The CNIL laid down four key criteria to be used when examining future requests, namely: (1) the use of biometric systems should be limited to the purpose of controlling access by a limited number of people to a zone with high security risks; (2) biometric systems should be proportionate to the purposes and the risks; (3) they should guarantee both the effective identification or authentication of individuals and the security of personal data; and (4) appropriate notice must be provided to individuals in compliance with French privacy and labor law. In 2007, the CNIL received 602 biometric authorization requests, among which 53 notifications concerned fingerprint-based identification systems, of which 32 were approved and 21 rejected.

The full text is available (in French) at: http://www.cnil.fr/index.php?id=2363&news

France: Suspended Jail Sentence Ordered for E-mail Spying

A Paris High Court decision of June 6, 2007 ordering for the first time a jail sentence for e-mail spying was recently made public. In November 2005, the managers of a French finance firm (Oddo et Cie) asked the police to investigate how information from confidential board meetings could have been leaked to the press. The police investigation revealed that a former external computer consultant used passwords of top managers collected during his stay at the firm to fraudulently enter the firm's computer and e-mail system. The Court found the consultant guilty of violating the secrecy of correspondence of two top managers and of fraudulent access to a protected computer system, and sentenced him to a six months' suspended jail sentence.

The Paris High Court decision is available (in French) at: http://www.legalis.net/breves-article.php3?id_article=2179

Ireland: DPA Issues Card Payment Guidance

On January 8, 2008, the Irish Data Protection Commissioner issued new guidance on the processing of credit and debit card payments in compliance with section 2(1) of Ireland's Data Protection Acts 1988 and 2003 regarding the collection and retention of personal data.

Under the guidance, where personal data stored on a card is collected for the purposes of a transaction, the purpose for this collection ends with completion of the payment for a product or service. Moreover, personal data obtained from a payment card for a particular transaction cannot be used subsequently for other transactions without the card holder's express consent. In addition, data controllers should adopt measures to ensure that information obtained for one purpose may not be accessed and used for another purpose. Finally, data controllers must specify the retention period of personal data and its purpose. Once retention is no longer required, the data must be deleted or securely stored (e.g., personal data collected from a card should be retained for a maximum of thirteen months).

The Guidance is available at: http://www.dataprotection.ie/viewdoc.asp?DocID=581&m=f

Netherlands: DPA Seeks More Enforcement Powers

On January 28, 2008, Dutch DPA chairman Jacob Kohnstamm issued a statement calling for more enforcement powers for his organization. He stated that: "[…] because of rapidly changing technology, we need to be able to take more direct action, such as investigations and fines […]". Recently, there has been an increase in data protection awareness in the Netherlands, in particular owing to the governmental debate on two possible laws likely to affect privacy: (1) a "pay-as-you-drive" law which will allow the government to track cars and trucks by camera in order to assess road taxes based on the distance driven; and (2) a proposal for a law that would create an electronic database of patient health records, accessible by medical personnel and insurance companies. The Dutch government so far has expressed no intention of increasing the DPA's powers.

The statement is available (in Dutch) at: http://www.cbpweb.nl/documenten/pb_20080128_dataprotectiedag.stm?refer=true

Spain Revises its Data Protection Legislation

On December 21, 2007, the Spanish Council of Ministers adopted a royal decree (Royal Decree 1720/2007) that fully implements Organic Law 15/1999 of December 13, 1999 on the protection of personal data. In particular, this Decree, which will enter into force on April 19, 2008: (1) brings within its scope security measures for paper files as well as electronic files; (2) categorizes personal data based on three levels of security: "basic" for any type of data, "medium" for criminal, fiscal and social security data, and "high" for sensitive information such as trade union membership, ideology, religion, beliefs, ethnicity, health and sexual life, and data collected by the police; (3) clearly sets out the responsibilities of the data controller and introduces more rigorous provisions for the processing of data by companies; and (4) provides that no DPA prior authorization is required for international data transfers to a country that guarantees an adequate level of protection.

The English version of Royal Decree 1720/2007 is available at: https://www.agpd.es/index.php?idSeccion=347

UK: ICO Takes Enforcement Action against Marks & Spencer

On January 23, 2008, the Information Commissioner's Office (ICO) took enforcement action against the supermarket chain Marks & Spencer (M&S) following the theft of a laptop computer containing pension information of its employees. The laptop was unencrypted and contained the personal information of 26,000 M&S employees. According to the ICO, pursuant to section 27(1) of the Data Protection Act 1998, it was the responsibility of the data controller to respect the seventh data protection principle, according to which *"appropriate technical and organisational measures shall be taken against unauthorised and unlawful processing of personal data and against accidental loss or destruction of or damage to personal data"*. M&S has until April 2008 to comply with the enforcement notice to encrypt their employees' personal data, failing which the ICO may initiate criminal proceedings.

The ICO decision is available at: http://www.ico.gov.uk/upload/documents/pressreleases/2008/mands_en_final.pdf

The enforcement notice is available at: http://www.ico.gov.uk/upload/documents/library/data_protection/notices/m_and_s_sanitiseden.pdf