

# **Data Protection and Rights Protection on the Internet: The Promusicae Judgment of the European Court of Justice**

**By**

**Christopher Kuner**

*Reprinted from*  
**European Intellectual Property Review**  
**Issue 5, 2008**

*Sweet & Maxwell Limited*  
**100 Avenue Road**  
**Swiss Cottage**  
**London**  
**NW3 3PF**  
*(Law Publishers)*

**THOMSON**  
  
**SWEET & MAXWELL**

This material was first published by Thomson/Sweet & Maxwell Limited in Christopher Kuner, "Data Protection and Rights Protection on the Internet: The Promusicae Judgment of the European Court of Justice," *European Intellectual Property Review*, Issue 5, 2008 and is posted/distributed by agreement with the Publishers.

# COMMENTS

Christopher Kuner\*

## Data Protection and Rights Protection on the Internet: The Promusicae Judgment of the European Court of Justice

 Copyright; Data protection; Disclosure; EC law; Electronic communications

The growth of electronic commerce has brought a corresponding increase in cyber crime and online fraud. These problems have grown so quickly, and have attained such vast dimensions, that unprecedented speed and effectiveness of enforcement are required to combat them. Budgetary pressures and lack of resources at the governmental level mean that in many cases, police and other law enforcement officials are not sufficiently equipped to deal with cyber crime and online fraud, making civil enforcement by private parties even more important. Effective civil enforcement often requires the processing of personal data, which in Europe is protected by data protection law.

On January 29, 2008, the European Court of Justice (ECJ) rendered its judgment in *Promusicae*,<sup>1</sup> the first case in which the Court has specifically dealt with the tension between data protection and online enforcement. In its judgment, the Court found that the European Union 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. The judgment illustrates the growing tension between the need to process personal data for civil enforcement purposes and the restrictions on processing such data under data protection law.

### The Promusicae case

This case was initiated by the Spanish rights-holder 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 peer-to-peer (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 authorised under Spanish law only for a criminal investigation or to safeguard public security and the national defence. The Spanish Court (Juzgado de lo Mercantil N° 5 de Madrid) 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. In particular, the Spanish Court asked the ECJ for a preliminary ruling as to whether the Member States are allowed under Community law to exclude the possibility of disclosing traffic data relating to copyright infringers in civil cases, while requiring such disclosure in criminal cases.

In an opinion delivered on July 18, 2007,<sup>2</sup> Advocate General Juliane Kokott concluded that it is compatible with Community law for Member States to exclude the communication of traffic data for the purpose of bringing civil proceedings against copyright infringements. Focusing first on the relationship between the different intellectual property (IP) directives involved in the case (including the E-Commerce Directive)<sup>3</sup> and their relationship to the relevant data protection directives,<sup>4</sup>

2 Opinion of Advocate General Kokott, the English version of which is available at <http://curia.europa.eu/juris/cgi-bin/form.pl?lang=en&newform=newform&Submit=Submit&alljur=alljur&jurcdj=jurcdj&jurtpi=jurtpi&jurftp=jurftp&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=275%2F06&ddatefs=&mdatefs=&ydatefs=&ddatefe=&mdatefe=&ydatefe=&nomusuel=&domaine=&mots=&resmax=100> [Accessed February 27, 2008].

3 The directives are Directive (EC) 2000/31 of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce in the Internal Market [2000] OJ L178/1 (the "E-Commerce Directive"); Directive (EC) 2001/29 of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society [2001] OJ L167/10 (the "Copyright Directive"); and Directive (EC) 2004/48 of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights [2004] OJ L157/45 (the "IP Enforcement Directive").

4 The directives are Directive (EC) 2002/58 of the European Parliament and of the Council of 12 July 2002 concerning the

\* Partner, Hunton & Williams, Brussels, e-mail [ckuner@hunton.com](mailto:ckuner@hunton.com).

1 *Productores de Música de España (Promusicae) v Telefónica de España SAU* (C-275/06) [2007] E.C.D.R. CN1, the English version of which is available at <http://curia.europa.eu/juris/cgi-bin/form.pl?lang=en&newform=newform&Submit=Rechercher&alljur=alljur&jurcdj=jurcdj&jurtpi=jurtpi&jurftp=jurftp&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> [Accessed February 27, 2008].

she found that all three IP directives are without prejudice to rules on data protection, including the E-Privacy Directive. However, the Advocate General also stressed that this does not mean that data protection automatically prevails over the objectives of the IP directives, since a balancing of the various interests and objectives must take place within the limits set by the data protection directives. The Advocate General stated that IP addresses should be considered to be traffic data and therefore personal data, and rejected arguments that Art.15(1) of the E-Privacy Directive, together with Art.13(1) of the Data Protection Directive, provide a legal basis for the disclosure of personal data in this case. She went on to state that it is permissible to disclose personal data to public authorities for enforcement purposes since they are directly bound by fundamental rights, which is not the case regarding private parties engaged in civil litigation.

In its judgment, the ECJ first considered whether the E-Privacy Directive precludes the Member States from laying down, with a view to ensuring effective protection of copyright, an obligation to communicate personal data which enable a copyright holder to bring civil proceedings.<sup>5</sup> The Court concluded that Art.15(1) of the Directive, in conjunction with Art.13(1) of the Data Protection Directive, does not preclude the Member States from laying down an obligation to disclose personal data in the context of civil proceedings [54], but that Art.15(1) cannot be interpreted as compelling the Member States to lay down such an obligation [55]. The Court then went on to find that Art.8(1) of the IP Enforcement Directive, Arts 15(2) and 18 of the E-Commerce Directive, and Arts 8(1) and (2) of the Copyright Directive do not require the Member States to lay down such an obligation [58 and 59]; the same is true, the Court found, about Arts 41, 42 and 47 of the Trade-Related Aspects of Intellectual Property Rights (TRIPS) Agreement [60].

The ECJ also found that Community law requires the Member States to transpose the above directives so as to allow a fair balance to be struck between the various fundamental rights involved (i.e. the right to respect for private life on the one hand and the rights to protection of property and to an effective remedy on the other hand) [65 and 68]. Furthermore, in transposition, the authorities and courts of the Member States must not only interpret their national law in a manner consistent with the directives, but must also make sure not to interpret the directives in a way which would conflict with such fundamental rights or with other general

processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L201/37 (the "E-Privacy Directive"); Directive (EC) 95/46 of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 (the "Data Protection Directive"); and Directive (EC) 2006/24 of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive (EC) 2002/58 [2006] OJ L105/54 (the "Data Retention Directive").

<sup>5</sup> Parenthetical references are to the paragraphs of the English version of the judgment.

principles of Community law, such as the principle of proportionality [70].

### Implications of the case

As the first ECJ case to evaluate the relationship between copyright protection and data protection, *Promusicae* is of fundamental importance. The definition of "personal data" under the Data Protection Directive and the E-Privacy Directive has been so broadly construed by the data protection authorities that nearly all types of data are subject to data protection law,<sup>6</sup> meaning that there will be inevitable conflicts between data protection law and enforcement needs. Personal data must be used in many types of enforcement that go beyond copyright issues: examples include hindering fraudsters from breaking into online accounts; monitoring persons who may commit fraudulent transactions in one Member State and then move to another one to avoid detection; and examination of employee emails by employers when the employee is suspected of violating law or policies. Until the *Promusicae* judgment, there had been a conspicuous lack of legal clarity regarding the extent to which personal data may be disclosed for the enforcement of private rights (including copyright enforcement), which has been reflected in differing decisions by national courts and data protection authorities over the last few years.<sup>7</sup>

In its judgment, the ECJ clarifies several important issues that had previously been unclear. Most importantly, the Court held that Community law neither forces Member States to allow the disclosure of personal data to private parties for civil enforcement purposes, nor does it preclude Member States from doing so, thus leaving the decision up to each Member State. By clarifying that Member States may allow the disclosure of personal data in civil cases, the Court's ruling allows the development of innovative mechanisms that respect data protection rights, while providing for effective enforcement of property rights. Such a mechanism could, for example, gradually escalate the response to acts of copyright infringement committed by subscribers to internet access services, with rights-holders monitoring traffic under certain conditions on P2P file-sharing networks in which certain subscribers, associated with a particular IP address, make copyrighted material available to others, and then requesting that the internet

<sup>6</sup> See Article 29 Working party, "Opinion 4/2007 on the concept of personal data" (WP 136, June 20, 2007).

<sup>7</sup> For example, the Belgian and French data protection authorities (DPAs) have reached different conclusions on the conditions under which parties may process IP addresses for enforcement purposes. Compare Belgian DPA, *Avis d'initiative n° 44/2001 concernant la compatibilité de la recherche d'infractions au droit d'auteur commises sur Internet avec les dispositions juridiques protégeant les données à caractère personnel et les télécommunications*, Commission de protection de la vie privée belge, 12 novembre 2001 with CNIL *Délibération 2006-294 du 21 décembre 2006 concernant la mise en oeuvre par l'Association de Lutte contre la Piraterie Audiovisuelle (ALPA) d'un traitement de données à caractère personnel ayant pour finalité principale la recherche des auteurs de contrefaçons audiovisuelles*. In addition, the CNIL Decision cited above finds that IP addresses are personal data, while the Paris Court of Appeal has ruled that they are not personal data (Cour d'appel de Paris, 13<sup>e</sup> chambre, section A, 15 mai 2007, currently under review by the Cour de Cassation Française).

service provider (ISP) forward to the user a notice reminding them of their duties under the subscription agreement with the ISP and of the broader consequences of copyright infringement. The ECJ's judgment at least leaves the door open to such mechanisms, as well as to self-regulatory schemes agreed between interested parties and data protection authorities (such as codes of conduct),<sup>8</sup> though their ultimate viability will depend largely on Member State law.

The judgment clarifies that Art.15(1) of the E-Privacy Directive (in conjunction with Art.13(1) of the Data Protection Directive) must be interpreted as allowing Member States to restrict the scope of obligations provided in certain articles of the E-Privacy Directive, when this is necessary to safeguard the rights and freedoms of others, including the right to property in civil proceedings [53]. This will allow Member States to adopt legislative measures restricting the scope of certain articles of the E-Privacy Directive in appropriate cases; the Advocate General's opinion had seemed to exclude this possibility ([85–89] of the Advocate General's opinion). The judgment will also help settle similar issues which have recently been brought before the Court in at least one similar case.<sup>9</sup>

In her opinion, the Advocate General contended that enforcement by public authorities necessarily results in greater respect for fundamental rights than does enforcement by private parties ([114] of the Advocate General's opinion). However, the Court's judgment does not refer to these contentions, and thus seems to place enforcement by private entities on the same footing as enforcement by public authorities, which is a more pragmatic and realistic view of the realities of online enforcement. Law enforcement authorities working to combat cyber crime and online fraud tend to be understaffed and underfinanced, and overwhelmed with many tasks. Furthermore, they often lack the technical expertise and equipment to effectively pursue copyright infringements.<sup>10</sup> In this situation, effectively combating online piracy requires substantial participation by private parties, who often have greater incentive to pursue violations than do public authorities. Effectively combating cyber crime does not present a stark choice between enforcement, either by public authorities or by private entities, but requires cooperation between both.<sup>11</sup> Furthermore, it is questionable whether data processing by public authorities necessarily results in

a higher level of data protection. Data processing by private entities is subject to the full panoply of data protection rules under the Data Protection Directive, the E-Privacy Directive, and implementing national laws,<sup>12</sup> whereas data processing by so-called "third pillar" public authorities (such as police and other law enforcement authorities)<sup>13</sup> is subject to a patchwork of national and local laws that provide varying degrees of data protection. At present, the European Union is attempting to reach agreement on a Council framework decision for data protection in the third pillar that would extend more uniform data protection rules to law enforcement entities. The debate surrounding this framework decision illustrates the generally low level of data protection that currently applies in the third pillar.<sup>14</sup>

The Court's judgment rightly emphasises the necessity of a balancing between the fundamental rights of data protection and the protection of property. The protection of intellectual property is recognised by Art.1 Protocol 1 of the European Convention on Human Rights<sup>15</sup> and Art.17 of the Charter of Fundamental Rights of the European Union, while data protection rights are recognised in Art.8 of the European Convention on Human Rights<sup>16</sup> and Art.8 of the Charter of Fundamental Rights of the European Union.<sup>17</sup> The judgment stresses that Member State courts and authorities (including data protection authorities) must balance these rights in the measures they take, and must strike a "fair balance" [68] between them. The Court further refers to the principle of proportionality in European law, which requires a balance to be struck between the means used and the intended aim of their actions,<sup>18</sup> thus strengthening the balancing requirement contained in the judgment. These conclusions should send a strong signal to Member States, national courts and authorities

8 Codes of conduct are envisioned, for example, in the Data Protection Directive (Art.27) and the E-Commerce Directive (Art.16).

9 See OGH Beschluss AZ: 4 Ob 141/07z vom 13. 11. 2007, in which the Austrian Supreme Court referred to the ECJ a case raising similar issues as *Promusicae*.

10 See Palmer, "Sleuths take on the cyber crooks", *Financial Times*, 3 January 2008, p.8, where the author states with regard to online enforcement that "police resources are limited" and police forces "are already stretched and tend to lack officers with specialist training needed to track Internet crime".

11 See European Commission, Communication from the Commission to the European Parliament, the Council and the Committee of the Regions towards a general policy on the fight against cyber crime, COM(2007) 267 final, p.7, where the Commission stated that, "shared private and public sector participation, based on mutual trust and a common objective of harm reduction, promises to be an effective way of enhancing security, also in the fight against cybercrime".

12 The European Commission has found, for example, that the Data Protection Directive (which applies to enforcement by rights-holders) "constitutes a general legal framework which fulfils its original objectives by constituting a sufficient guarantee for the functioning of the Internal Market while ensuring a high level of protection". European Commission, Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, COM(2007) 87 final, p.9.

13 See Art.3(2) of the Data Protection Directive.

14 See Third opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters of April 27, 2007 (2007/C 139/01), p.2:

"The EDPS is disappointed about the content of the text presented by the German Presidency. The text does not fulfil expectations for the following reasons: The text weakens the level of protection of the citizens; in many aspects even falls below the level of protection afforded by Convention 108; adds new complexities to the dossier; the legislative quality of the text is unsatisfactory; the low level of protection afforded by the proposal cannot properly serve the creation of an area of freedom, security and justice."

15 See for example, *Anheuser-Busch Inc. v Portugal* (73049/01) [2006] E.T.M.R. 43; (2007) 44 E.H.R.R. 42 at [72].

16 See for example, *Rotaru v Romania* (28341/95) 8 B.H.R.C. 449 at [46].

17 Charter of Fundamental Rights of the European Union [2000] OJ C364/1.

18 See K. Lenearts and P. Van Nuffel, *Constitutional Law of the European Union*, 2nd edn (Sweet & Maxwell, 2005), pp.109–112.

that neither data protection nor IP protection should be given precedence over the other. This should hopefully lead to more innovative mechanisms being developed for reconciling these two fundamental interests.

Member States already differ in the extent to which they allow the disclosure of personal data for IP enforcement purposes.<sup>19</sup> By allowing Member States to refuse the disclosure of personal traffic data related to copyright infringements for the purpose of bringing civil proceedings, the ECJ's judgment may lead to a further fragmentation of the law, in which some Member States allow such use but others do not. In other areas (such as the detection of payment fraud online), European law has created a more uniform legal basis for the processing of personal data,<sup>20</sup> and a similar European approach should be taken with regard to the enforcement of IP rights. Indeed, the internet is a global medium, and substantial legal uncertainty can arise regarding issues such as which Member State law should apply to a particular enforcement action. Thus, it would be preferable for a pan-European approach to be taken, under which online enforcement would be possible in all Member States under the same legal conditions; such an approach would also reduce the risk of forum-shopping. However, following the *Promusicae* judgment, amendment of at least the E-Privacy Directive would be required to create a legal basis for such an approach.

### Conclusions

*Promusicae* is the first ECJ case to examine the conflict between IP enforcement and data protection rights. The Court's judgment makes it clear that European Union law neither compels the disclosure of personal data for civil enforcement purposes, nor does it prohibit it, and thus turns the focus of attention on this issue back to the Member State level. However, in the internet age, this kind of national approach is bound to lead to difficulties. Thus, it would be preferable for a pan-European approach to be developed, either as binding law by the European legislator, or in the scope of a self-regulatory scheme. In the meantime, the Court's

19 Compare, for example, the following cases: Italy: *Techland Sp. Z O.O. e Peppermint Jam Records GmbH contro Wind Telecomunicazioni S.p.A.*, Tribunale di Roma, Sezione IX civile, ordinanza del 14 luglio 2007 Giudice Costa, in which the Court stated that identity disclosure requests are unacceptable because of the protection afforded to the secrecy of electronic communications between private parties, which is granted by the Italian Constitution as a fundamental right; Netherlands: Hoge Raad, November 25, 2005, LJN:AU 4019, *Lycos/Pessers*, in which the Dutch Supreme Court ruled that Dutch privacy law does not necessarily prohibit the disclosure of personal data by ISPs to third parties, and whether or not such disclosure is allowed depends on the specific circumstances of the case; UK: *Totalise Plc v Motley Fool Ltd* [2001] EWCA Civ 1897, in which the House of Lords held that website operators should disclose the identity of wrongdoers (in this case an offender posting defamatory material to a website operator's discussion board).

20 See Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market [2007] OJ L319/1, Art.79 of which reads: "Member States shall permit the processing of personal data by payment systems and payment service providers when this is necessary to safeguard the prevention, investigation and detection of payment fraud. The processing of such personal data shall be carried out in accordance with Directive 95/46/EC."

emphasis on a balancing between data protection rights and IP rights provides useful clarification, which should help guide both public authorities and private entities in dealing with online enforcement issues.

Nikos G. Prentoulis\*

## The Omega Ruling: Trade Mark Co-existence Agreements in the Tension Between "Public" and "Private" Trade Mark Law

LT Co-existence agreements; Confusion; EC law; Trade marks

### Co-existence agreements and trade mark practice

Trade mark law is generally understood and taught as a child of the private law family. Why then would a court choose to disregard a trade mark co-existence agreement, one of the most classic demonstrations of the force of private will within trade mark law? The CFI's recent judgment on the *Omega* case<sup>1</sup> serves to trigger the discussion of an interesting aspect of the balance between public and private law considerations within the trade mark law realm.

Co-existence agreements are a well-known and accepted instrument of trade mark dispute resolution. In the World Intellectual Property Organisation's (WIPO) own words:

"Trademark coexistence describes a situation in which two different enterprises use a similar or identical trademark to market a product or service without necessarily interfering with each other's businesses. This is not uncommon."<sup>2</sup>

Their recognition does not only arise from legal practice. The EC Directive 89/104 on the approximation of the trade mark law of the EU Member States, expressly provides for the validity of such agreements, though—oddly enough—no such reference can be found in the EC Regulation 40/1994 on the Community trade mark. The well-known and frequently cited case of *Apple Corps*, the record label founded by the Beatles, and *Apple Computer*<sup>3</sup> is a lucid example of both the

\* Attorney at Law, LL.M., Partner, Georgouleas, Davrados & Prentoulis, Athens, Greece.

1 Court of First Instance of the European Communities, (T-90/2005) *Omega SA v OHIM - Omega Engineering Inc*, judgment of November 6, 2007, available at <http://curia.europa.eu/juris/cgi-bin/form.pl?lang=en&newform=newform&Submit=Submit&alljur=alljur&jurcdj=jurcdj&jurtpi=jurtpi&jurftp=jurftp&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=t-90%2F05&ddatefs=&mdatefs=&ydatefs=&ddatefe=&mdatefe=&ydatefe=&nomusuel=&domaine=&mots=&resmax=100> [Accessed February 27, 2008].

2 Tamara Nanayakkara, "Trademark Coexistence", *WIPO Magazine*, 2006, p.18.

3 *Apple Corps Limited v Apple Computer Inc.* [2006] EWHC 996 (Ch).

This material was first published by Thomson/Sweet & Maxwell Limited in Christopher Kuner, "Data Protection and Rights Protection on the Internet: The Promusicae Judgment of the European Court of Justice," *European Intellectual Property Review*, Issue 5, 2008 and is posted/distributed by agreement with the Publishers.