The implications of copyright infringement on the right to data protection in European Union law in the context of peer-to-peer technology

Introduction

The advantages derived from the “brave new digital world that is the information society”\(^1\) are too numerous and varied to list. However, one innovation that has had an extraordinary impact on the music industry, and music distribution in particular, is the invention of peer-to-peer (P2P) file-sharing networks. These networks allow users of certain software to enable other users of the same software to have access to a portion of their resources (for instance, disk storage, network bandwidth or, most commonly, media files). This system generally functions without any central coordination, hence the name “peer-to-peer”. P2P file-sharing owes its popularity in part to the invention of the mp3 music format in the late 1990’s and to the subsequent growth of systems like Napster, which made digital file-sharing possible.

While file sharing is not illegal as such, the sharing of copyright-protected materials without authorisation is. Consequently, this innovation, which has proven highly advantageous for consumers, is also challenging established legal rights, in situ copyright. As a result, legislatures have sought to introduce new solutions to tackle the problems such innovation gives rise to. For instance, in the European Union, the “E-commerce Directive”\(^2\) necessitates that Member States place an obligation on Internet Service Providers (ISPs) to inform competent public authorities of alleged illegal activity undertaken by recipients of their services and, at the request of these public authorities, to provide information enabling the identification of the alleged offenders.\(^3\) Moreover, in several countries across Europe, legislative measures have been enacted to enable copyright holders to gain access to the information necessary to identify and prosecute copyright infringers. Such legislation is necessary as without it the right to property of copyright holders, as well as their right to an effective remedy, would be breached. However, by revealing the identity and personal details of alleged copyright infringers ISPs infringe the right to privacy of these alleged infringers, in particular their right to data protection. By pitting the right to property

---


\(^3\) Article 15(2) of the E-Commerce Directive
and the right to an effective remedy of copyright owners\textsuperscript{4} against the right to privacy and data protection of those alleged infringers whose coordinates are revealed, such legislative measures are fraught with difficult legal issues.

This paper sets out to consider how, under European law, the right to data protection is, and should be, reconciled with the right to property in the context of P2P file-sharing. To this end, the relevant European legal landscape will be set out in section I. Section II will outline the Promusicae\textsuperscript{5} judgment of the European Court of Justice (ECJ) which considered how these rights could be reconciled and will also consider the merits of this judgment. Section III will suggest how these rights should best be reconciled in practice in the aftermath of Promusicae. A brief conclusion will then be reached.

I. The European legal framework

i) European primary law

The European Community (EC) Treaty referred to data protection only indirectly in its Article 286 which stated that “Community acts on the protection of individuals with regard to the processing of personal data and the free movement of such data shall apply to the institutions and bodies set up by, or on the basis of, this Treaty.” Meanwhile, the same Treaty contained no substantive legal provision concerning Intellectual Property (IP) law.

The Treaty for the Functioning of the European Union (TFEU or Lisbon Treaty) has altered this situation significantly. Chapter 3 of the Treaty which concerns the “Approximation of Laws” now explicitly refers to IP in its Article 118. Article 118 TFEU reads as follows: “In the context of the establishment and functioning of the internal market, the European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall establish measures for the creation of European intellectual property rights to provide uniform protection of intellectual property rights throughout the Union and for the setting up of centralised Union-wide

---

\textsuperscript{4} For the purposes of this paper, this issue will be conceptualised from a human rights perspective. I will therefore argue that copyright should be enforced in order to protect the right to property of copyright holders. However, this scenario could equally be considered from a broader perspective by examining how best to taking into consideration the benefits which flow from the underlying public-good qualities of intellectual property rights.

\textsuperscript{5} C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España [2008] ECR I-271

New Technologies and the Right to Privacy
authorisation, coordination and supervision arrangements”. This provision provides a clear mandate for European legislation in the field and serves to reinforce the importance of harmonised IP laws to the European single market. Moreover, data protection has now been given more explicit recognition in the TFEU, appearing in its “Provisions of General Application”. Article 16 TFEU reiterates what was previously stated by Article 286 EC but also provides that “Everyone has the right to the protection of personal data concerning them”; it therefore provides for a directly effective\(^6\), right to data protection.

Finally, since the entry into force of the TFEU the human rights credentials of the EU have been significantly reinforced. Not only has the Union become a signatory of the European Convention of Human Rights\(^7\) (ECHR) but its Charter of Fundamental Rights (Charter) is now legally binding primary law. This Charter sets out a right to privacy and a separate right to data protection in its Articles 7\(^8\) and 8\(^9\). Furthermore, Article 17 of the Charter sets out the right to property. Article 17(2) is dedicated in particular to IP “laconically”\(^10\) stating that “Intellectual property shall be protected”. It should also be noted that Article 52(3) of the Charter stipulates that when rights set out in the Charter correspond to those guaranteed by the ECHR, “the meaning and scope of those rights will be the same as those laid down in the ECHR”. This provision therefore obliges the ECJ to abide by the jurisprudence of the European Court of Human Rights (ECtHR) when relevant\(^11\).

\(^6\) Article 16 TFEU is clear, precise and unconditional and therefore fulfils the conditions for direct effect. The European Data Protection Supervisor (EDPS) has indicated that this provision is directly effective in his speech entitled “Data Protection in the Light of the Lisbon Treaty and the Consequences for Present Regulations” delivered at the 11\(^\text{th}\) Conference on Data Protection and Data Security in Berlin on 8 June 2009. Viewed at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2009/09-06-08_Berlin_DP_Lisbon_Treaty_EN.pdf

\(^7\) The right to privacy is set out in Article 8 of the ECHR and data protection has been recognized as one facet of privacy by the jurisprudence of the European Court of Human Rights (ECtHR).

\(^8\) Article 7 provides that “Everyone has the right to respect for his or her private and family life, home and communications”

\(^9\) Article 8(1) stipulates that “Everyone has the right to the protection of personal data concerning him or her”. This right is elaborated upon in Article 8(2) which provides that the data “must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law” and that “everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified”


\(^11\) It is interesting to note that Article 52(3) also states that it “...shall not prevent Union law providing more extensive protection”.

New Technologies and the Right to Privacy
ii) European secondary law

In the present context, the data protection of internet users is guaranteed in Europe by both the Data Protection Directive\textsuperscript{12} and the E-Privacy Directive\textsuperscript{13}. The Data Protection Directive sets out the general principles which must be applied to data processing in order to make it lawful. The E-Privacy Directive complements this general Directive by setting out specific rules to address data protection issues arising with regard to new technologies and electronic communications. Copyright is regulated by a variety of Directives at European level; in particular, the E-commerce Directive\textsuperscript{14}, the Directive on harmonization of certain aspects of copyright and related rights in the information society\textsuperscript{15} (the Information Society Directive) and the Directive on enforcement of IPRs.\textsuperscript{16} While these latter Directives do not refer to human rights considerations, it should be noted that both the Data Protection Directive and the E-Privacy Directive refer explicitly to these concerns. The third recital of the Data Protection Directive provides that “...the establishment and functioning of an internal market (…) require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded” (emphasis added). Similarly, the second recital of the E-Privacy Directive states that it “In particular, this Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of that Charter”. Nevertheless, even without these explicit references it is clear that as a result of the binding provisions of the Charter, these Directives must be interpreted in the light of this human rights framework. Indeed, the Court factored human rights considerations into its Promusicae judgment of its own volition as will be seen presently.

\textsuperscript{12} European Parliament and Council Directive 95/46/EC 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 (Official Journal L 281 of 23.11.1995)


\textsuperscript{14} Supra note 2


iii) Pertinent case-law of the ECJ

The right to property in EU law

Despite initial reluctance\(^{17}\), the right to property was acknowledged by the ECJ in *Nold v. Commission*.\(^{18}\) The right to property has, in particular, been invoked before the ECJ to challenge measures taken in the context of the Common Agricultural Policy\(^{19}\) and for the harmonisation of the common market\(^{20}\). The Court acknowledged that the right to property encompasses the right to intellectual property in its *Laserdisken*\(^{21}\) judgment where it held that a potential restriction on the freedom to receive information as a result of the exhaustion doctrine may be “justified in the light of the need to protect intellectual property rights, including copyright, which form part of the right to property”\(^{22}\). The Court had consistently upheld the right, which is a general principle of European law, and emphasises that the right is derived from the constitutional traditions common to the Member States\(^{23}\) and from guidelines supplied by international human rights treaties. The ECHR has often been singled out as having “special significance” in this regard.\(^{24}\) However, the ECJ has also consistently emphasised that the right to property is not absolute and must be viewed in relation to its social function.\(^{25}\) Consequently, measures which restrict this right which have Community objectives of general interest and that do not constitute a disproportionate and intolerable interference in relation to the aim pursued or impair the very substance of the right guaranteed are deemed permissible.

\(^{17}\) According to Becker this is because “[The ECJ] had initially perceived fundamental rights (and the Right to Property in particular) as an obstacle to market integration holding that ‘Community law...does not contain any general principle, express or otherwise, guaranteeing the maintenance of vested rights.’”. See Becker, “Market Regulation and the ‘Right to Property’ in the European Economic Constitution”, *Yearbook of European Law* 2007, 26, p.255, 2008


\(^{19}\) See for instance, C-20/00 and 64/00, *Booker Aquaculture and Hydro Seafood v. The Scottish Ministers* [2003] ECR 1 - 7411

\(^{20}\) See for example, C-154/04 and C-155/04, *R. v. Secretary of State for Health ex parte Alliance for Natural Health* (2005) ECR I-6451

\(^{21}\) C-479/04, *Laserdisken* [2006] ECR I-8089

\(^{22}\) Ibid., para. 65

\(^{23}\) The Court has not analysed Member States’ constitutional provisions regarding the right to property in its case-law. However, in His Opinion in Booker Aquaculture (supra note 19), Advocate General Mischo considered these provisions in some depth (paras. 116 to 124).

\(^{24}\) Supra note 19, para. 65

Despite constant affirmation that the right to property is protected under European law, it has proven to be notoriously difficult for applicants to successfully invoke this right against the European Union. For instance, in Flughafen the applicant, the managing board of an airport, challenged a measure, taken to implement a Community Directive, which prohibited it from collecting access fees to the ground-handling market. The Court held that as this measure did not deprive the managing body of the possibility to exploit its property in such a way as to make a profit, the measure did not infringe the applicant’s right to property. Indeed, it was noted by Tridimas in 2006 that the Court had not to date upheld a claim based on an infringement of the right to property. Tridimas observed that the Court preferred to base its reasoning on other rights, such as the principle of equality or legitimate expectations when they are invoked in tandem with the right to property. This is perhaps because these rights are by now more firmly established in the European Union legal order. Tridimas also remarked that the Court had not given specific guidelines as to what type of measure could constitute an infringement of the right to property. He concluded from the case law that “...a right may be deprived of much of its economic value without amounting to a breach of the right to property” and that therefore “it seems the purpose of the right is to prohibit expropriation”.

However, the Court held for the first time in the case of Kadi that the applicant’s right to property was infringed by a Community measure temporarily restricting the exercise of that right. In Kadi the Court considered whether a freezing measure imposed upon Mr. Kadi impaired the very substance of his right to property. Following the analytical framework used by the ECtHR, the ECJ noted that the freezing measure in question was a “temporary precautionary measure” yet the exercise of Mr. Kadi’s right to property was undeniably restricted. The

26 This has prompted Becker (supra note 17) to remark that “Most decisions still only pay lip service to its effective protection”.
27 C-363/01, Flughafen Hannover-Langenhagen [2003] ECR I-11893
28 Ibid., para. 55
31 Pre-Kadi, Advocates General showed a greater willingness to rely on the right to property when Community measures were challenged. In C-376/98, Germany v. Parliament [2000] ECR I-8419, the Advocate General considered that the challenged Directive imposed restrictions which were not necessary to achieve the internal market objectives pursued, it was therefore disproportionate and the interference with the right to property could not be justified.

New Technologies and the Right to Privacy
restriction was deemed to be a considerable one given that the freezing measure was of general application and that it applied to Mr. Kadi since October 2001. Having established the existence of a restriction the ECJ then turned to the question of justification, again referring to ECtHR jurisprudence. The Court noted that freezing measures are not per se disproportionate as they pursue the general interest of fighting against terrorist threats to peace and security and thus held that in principle the restrictions affecting Mr. Kadi might be justified. The Court then queried whether on the facts of the case Mr. Kadi’s right to property had been respected. In particular, the Court examined whether the appellant had a reasonable opportunity to present his case to the authorities, a procedural requirement inherent in Article 1 of Protocol 1 ECHR. The Court found that the contested regulation did not enable Mr. Kadi to present his case to the competent authorities when his property right had been significantly restricted and therefore concluded that the imposition of the restrictive freezing measures constituted an unjustified restriction of his right to property.

Since Kadi the Community judicature has found similar violations of the right to property in Hassan and Omar Mohammed Othman. However, it is questionable whether this line of jurisprudence marks a general lowering of the threshold to establish an infringement of the right to property under European law. Rather, what is notable about these cases is that the Court has placed emphasis on the paramount importance of the procedural requirements inherent in Article 1 of Protocol 1 ECHR and was ready to find a breach when they are not respected. Interestingly, this follows the development of the right to property under Article 1 of Protocol 1 ECHR with

---

32 Ibid., para. 358
33 The Court also referred to its own judgment in Bosphoros (supra note 25) where it was held that “the importance of the aims pursued by a Community act is such as to justify negative consequences, even of a substantial nature, for some operators, including those who are in no way responsible for the situation which led to the adoption of the measures in question, but who find themselves affected, particularly as regards their property rights”.
34 In C-266/05 P Sison [2007] ECR I-1233, which pre-dates the ECJ’s Kadi judgment, the applicant’s claim was rejected as the freezing measure “unlike confiscation, does not affect the very substance of the right of the person concerned to property in the assets in question but only the use and therefore the availability of the assets” (para.245).
35 In T-390/08, Bank Melli Iran [2009] (nry) the argument based on the right to property was rejected as the restriction in question was deemed to be proportionate; the CFI held that those restrictions concern only part of the applicant’s assets and the Regulation provides for certain exceptions allowing the entities affected by fund-freezing measures to meet essential expenditure.
36 C-399/06 P, Hassan v Council and Commission, OJ 2006 C 294/30
37 T-318/01, Omar Mohammed Othman v Council and Commission (2009) nyr
regard to intellectual property. As Helfer has noted on both occasions to date when the ECtHR has had the opportunity to consider state interferences with IP, it has concluded that the exercise of rights was controlled but that right holders were not completely deprived of their rights and it has not found in their favour. However in one of these cases, Anheuser-Busch, the Grand Chamber of the ECtHR made the following statement:

“Even in cases involving litigation between individuals and companies, the obligations of the State under Art.1 of Protocol 1 entail the taking of measures necessary to protect the right of property. In particular, the State is under an obligation to afford the parties to the dispute judicial procedures which offer the necessary procedural guarantees and therefore enable the domestic courts and tribunals to adjudicate effectively and fairly in the light of the applicable law”.

This statement mirrors the finding of the ECJ in Kadi and as Helfer observes it may have important implications as “the ECtHR may interpret these due process guarantees as requiring member states to provide statutory, administrative and judicial mechanisms to enable intellectual property owners to prevent private parties from infringing their protected works”. Thus, there is potential for the ECJ jurisprudence to develop in the same manner and to come to the assistance of aggrieved copyright holders who seek the personal data of alleged infringers from ISPs.

The right to data protection

Following the enactment of the Data Protection Directive, which explicitly seeks to protect the privacy of individuals when data is processed, a significant body of data protection case-law has

---

41 Supra note 38, p. 32
42 Supra note 12
emerged. Given the relevance of this case-law to the issue of whether the personal data of alleged copyright infringers may be processed, it will be briefly considered.

In Österreichischer Rundfunk the Court was asked to consider whether Austrian legislation which requires the communication of the salaries of senior officials to the national audit body to enable it to monitor the reasonableness of those salaries was contrary to the Data Protection Directive. The Court cited Article 8 ECHR before systematically considering whether there had been a violation of this provision and whether it was justified. The Court held that while the mere recording by an employer of remuneration data concerning an employee does not constitute an infringement of the latter’s privacy, the subsequent transferral of such information to third parties does. The Court then referred to the issue of justification, citing jurisprudence of the ECtHR, and noted that there may be serious consequences on the job market for those whose names are published alongside their salaries. The Court concluded by stating that the measure can only be justified if the national court deems it necessary and appropriate to the aim of keeping salaries within reasonable limits to publish the names of those concerned.

In Lindqvist, the Court considered whether the act of uploading information on an internet page concerning various persons and identifying them for non-profit purposes constitutes data processing within the meaning of the Data Protection Directive. The applicant argued in the case that such an act was a manifestation of her freedom of expression as protected by Article 10 ECHR. The Court did not address this argument. It simply noted that Mrs. Lindqvist’s freedom of expression must be weighed against the protection of the private lives of those whose data she posted on her site. The Court then however opined that it is for Member States to not only interpret their laws in a way consistent with the Data Protection Directive but also to make sure

---

43 Despite the fact that the Data Protection Directive refers explicitly to the protection of privacy as one of its objectives, the right to data protection and the right to privacy should not be conflated as is illustrated by the Charter which provides for both rights individually. As has been highlighted by Brouwer, data protection is motivated by more than privacy concerns, for instance the rule of law and the principle of good administration necessitate such rules (see Brouwer, Digital Borders and Real Rights - Effective Remedies for Third-Country Nationals in the Schengen Information System, Martinus Nijhoff Publishers, 2008, Leiden).

44 C-139/01 Österreichischer Rundfunk and Others [2003] ECR I-4989

45 Interestingly the Advocate General in this case refused to consider the compatibility of the national legislation in question with the Data Protection Directive as he did not consider it to fall within the scope of the Community jurisdiction on the grounds that there was no link with Community Internal Market legislation.

46 C-101/01 Bodil Lindqvist [2003] ECR I-12971

New Technologies and the Right to Privacy
that they do not rely on an interpretation of the Directive that would conflict with other rights protected by the Community legal order.\textsuperscript{47}

In \textit{Satamedia}\textsuperscript{48}, Satakunnan collected personal data relating to 1.2 million persons who earned over a certain threshold from the Finish tax authorities. Abstracts from the information collected were then published in local editions of a national newspaper. These abstracts included the names, earnings to the nearest EUR 100 and wealth tax levied on these people. Satakunnan then transferred this information on CD-ROM discs to Satamedia so that the latter could disseminate it via text message. The Finnish Data Protection Authority’s refusal to prevent Satamedia from providing this messaging service was challenged before the Courts and culminated in a preliminary reference to the ECJ. The ECJ noted that the objective of the Data Protection Directive is to provide for the free flow of personal data whilst protecting the fundamental rights of persons, in particular privacy, with regard to data processing\textsuperscript{49}. The Court noted that this objective must be reconciled with the right to freedom of expression and that Article 9 of the Directive provides the means to do this by providing for derogations to the Directive when data is processed for “journalistic purposes” or for “the purpose of artistic or literary expression”. The Court concluded that the activities in question could constitute “journalistic activities” if “their object is the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them”\textsuperscript{50}. It was for the national court to consider this on the facts.

In \textit{Bavarian Lager}\textsuperscript{51} what was at stake was the refusal by the Commission to grant the applicant access, in accordance with the Access to Documents Regulation, to the names of participants in the Commission’s decision-making procedure. Both the Court of First Instance (now “General Court”) and the Advocate General, whose Opinion was sought following the appeal of the case,  

\begin{itemize}
\item[\textsuperscript{47}] Para. 87
\item[\textsuperscript{48}] C-73/07, \textit{Tietosuojavaltuutettu v. Satakunnan Markkinapörssi OY, Satamedia}, [2008] (nyr)
\item[\textsuperscript{49}] Para. 52
\item[\textsuperscript{50}] In her Opinion Advocate General Kokott proposed that the term “journalistic purposes” be restrictively construed. She suggested that information that is disseminated for the purposes of informing public debate, as opposed to information that is published for the “sole purpose of satisfying the curiosity of a particular readership”, should fall within the scope of this term (paras. 69 to 74). This interpretation of the notion of journalistic purpose is preferable to the interpretation favoured by the Court.
\item[\textsuperscript{51}] Case T-309/97 \textit{Bavarian Lager v Commission} [1999] ECR II-3217
\end{itemize}

New Technologies and the Right to Privacy
interpreted “privacy” in different ways. The CFI reached the conclusion that the disclosure of the names in question “does not lead to an interference with the private life of the persons who participated in the meeting and would not undermine the protection of their private life and the integrity of their person”. The Advocate General was however of the opinion that the disclosure of the names of the persons concerned, even in the context of business relations, constituted a potential interference that breached Article 8 ECHR.

Huber concerned an Austrian national who was living and established in Germany. His personal details were stored in a database with those of other non-nationals in Germany. Mr. Huber challenged the retention and processing of this data on the grounds that it was discriminatory (as such a database does not exist in relation to German nationals) and contrary to the principle of necessity as set out in the Data Protection Directive. The Court emphasised that the principle of necessity should ensure that there is a uniformly high level of protection of personal data throughout the European Union. It held that a system such as that in place in Germany that has as its aim to support national authorities responsible for applying legislation on the right of residence does not comply with the principle of necessity unless it contains only the data necessary to apply that legislation and its centralised nature guarantees that it will be applied more effectively. The Court referred these issues back to the national court for adjudication. Although the national court did not refer to the right to privacy in the questions referred, it is noteworthy that unlike the Advocate General, who highlighted that “...when a national measure is incompatible with Article 8 of the Convention, it also fails to pass the threshold of Article 7(e) of Directive 95/46”, the Court made no reference to the right to privacy or the ECHR when reaching this finding.

52 The interpretation of Article 8 ECHR was not the only point on which the reasoning of the Advocate General and the General Court differed. The Advocate General proposed that in this case, no clash existed between the right to data protection and the right of access to documents. According to the Advocate General, the document sought did not fall within the scope of the Data Protection. She noted that the main purpose of the minutes was not to collect personal data; the inclusion of personal data was incidental. Moreover, the data was not processed “partly or wholly by automatic means” nor did it form part of a filing system. It was only in considering alternative options to her preferred solution in this case that the Advocate General considered Article 8 ECHR.

53 Para. 153

54 Case C-524/06 Heinz Huber v Bundesrepublik Deutsch land [2008] (nyr)

55 Article 7(e) of the Data Protection Directive sets outs this principle. It provides that “Member States shall provide that personal data may be processed only if: (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed be”.

New Technologies and the Right to Privacy
A number of general conclusions can be reached on the basis of this case-law. First, the European Union judicature (that is the General Court, the ECJ and its Advocates General) have demonstrated an inconsistency with regard to when and how Article 8 ECHR should be applied. They have been inconsistent as to when it should be applied as it is not even referred to in some judgements, for instance *Huber* despite the fact that the Advocate General highlighted its relevance. The differing application of Article 8 ECHR to the same facts by both the General Court and the Advocate General in *Bavarian Lager* is an example of how they have been inconsistent when considering how Article 8 ECHR is applied. Second, it is arguable that in *Satamedia* the Court did not grant sufficient weight to the right to privacy vis-a-vis another ECHR rights, in that case the freedom of expression. Indeed, Oliver has noted that in *Satamedia* “the Court’s failure to confine the concept of ‘journalism’ to matters of public concern seems hard to reconcile with either the letter or the spirit of the ECtHR provision on freedom of expression”. It will be therefore interesting to see how the Court will deal with future conflicts between the right to data protection and other Convention rights, particularly those rights that are less well-established for instance the right to property. Third, even in this newly emerging area of law where fundamental rights must frequently be balanced, the ECJ has not given national courts sufficient guidelines to determine how the balance should be struck to sufficiently guarantee the right to privacy. This is again evident in *Satamedia* prompting Oliver to suggest that “the Court’s open-ended ruling appears to allow national courts virtually unfettered discretion in defining the concept of journalism”. The consequences of such a laissez-faire approach should not be underestimated; not only may it hinder the free movement of personal data within the European Union, it will also lead to differing standards of protection of the right to privacy throughout the Union. Therefore although the Court placed considerable emphasis on the goal of guaranteeing equivalent protection for personal data across Europe, its own jurisprudence seems to be endangering the achievement of this goal. It is against this backdrop that we must turn to consider the ECJ’s judgment in *Promusicae*, where the Court was provided with an opportunity to consider how best to reconcile the potential conflict between data protection and copyright enforcement.

---

56 Oliver, “The protection of privacy in the economic sphere before the European Court of Justice” 2009 Common Market Law Review 46 1443
57 Ibid., p. 1463
II. The ECJ’s Promusicae judgment

At issue in Promusicae was whether European law precludes Member States from adopting national legislation that obliges ISPs to provide the personal data of alleged copyright infringers to copyright holders in order to facilitate civil proceedings. Somewhat unhelpfully, the ECJ held that European law neither precludes nor compels Member States to place such an obligation on ISPs.

The facts of the case were as follows. Promusicae, an association of music producers and publishers, lodged an application before a Spanish court against Telefónica, an ISP, requesting that Telefónica disclose the names and addresses of a number of its clients. Promusicae had data to indicate that acts of copyright infringement had been committed from certain IP addresses. However, as IP addresses are similar to a telephone number, Promusicae needed the names and addresses of the IP address holders in order to commence civil proceedings against them. The Spanish Court questioned whether European law, and three Directives in particular, requires Member States to oblige ISPs to communicate personal data to Intellectual Property Right (IPR) holders to facilitate civil proceedings for IP enforcement. The three Directives referred to by the national court were the aforementioned E-Commerce Directive, the Directive on harmonization of certain aspects of copyright and related rights in the information society and the IPR enforcement Directive.

The ECJ reformulated the question asked by the referring Court by firstly considering whether European Data Protection law, in situ the Data Protection Directive and the E-Privacy Directive, precludes a Member State from laying down such an obligation, secondly whether the three Directives referred to by the Spanish court require that such an obligation is laid down and thirdly whether other European law rules, such as the Charter of Fundamental rights, have an impact on the conclusions reached for the first two questions.

The ECJ noted that the E-Privacy Directive ensures the confidentiality of electronic communications on public networks and, in principle, prohibits the storage of data for purposes other than billing without the consent of the user. However, under Article 15(1) of the Directive Member States may impose restrictions on this general confidentiality obligation when they “constitute a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention,
New Technologies and the Right to Privacy

investigation, detection and prosecution of criminal offences or of unauthorised use of the
electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC”. The
Court analysed this provision and held that it does not concern situations that include the
bringing of civil proceedings, as it concerns activities of the State unrelated to the field of
activity of individuals (national and public security and defence) or the prosecution of criminal
activities. It agreed with the Advocate General and the European Commission that the
“unauthorized use of the electronic communication system” refers to activities which call into
question the integrity or security of the system as such, for instance unauthorized surveillance of
communications.58 With regard to the reference to Article 13(1) of the Data Protection Directive,
the ECJ noted that Article 13(1) also allows Member States to restrict the confidentiality
obligation when such a restriction is necessary to “protect the rights and freedoms of others”.
The Court then held that Article 15(1) “must be interpreted as expressing the Community
legislature’s intention not to exclude from [its] scope the protection of the right to property or
situations in which authors seek to obtain that protection in civil proceedings”. The Court
therefore concluded that the E-Privacy Directive does not preclude the possibility of Member
States laying down an obligation to disclose personal data in the context of civil proceedings, nor
does it however compel Member States to set forth such an obligation.

The ECJ then considered whether the three Directives referred to by the referring Court
necessarily lead to such an obligation on ISP’s to disclose the IP address-holder’s data. The ECJ
found that all three of the Directives contain provisions stating that their provisions cannot affect
the requirements of the Data Protection Directive and therefore concluded that the IP Directives
do not compel ISPs to provide the personal data necessary to commence civil proceedings.

Finally the Court examined whether Articles 17 and 47 of the Charter, which set out the rights to
IP and an effective remedy respectively, are infringed as a result of such a reading of the three IP
Directives. The ECJ recalled that both the right to property, including intellectual property, and
the right to an effective remedy constitute general principles of Community law. The Court noted
however that these rights must be balanced against the right to the protection of personal data
and private life.59 The Court declared that the mechanism that allows these rights and interests to

58 Para. 52
59 It is noteworthy that the Court seems to conflate the right to data protection and the right to privacy. “However,
the situation in respect of which the national court puts that question involves, in addition to these two rights, a
be balanced is contained in the E-privacy Directive, in the IP Directives referred to by the national court and in national transposition measures. From this simple observation the Court therefore reached the conclusion that there is neither an obligation nor a prohibition on Member States to compel ISPs to provide personal data to third parties for the purposes of civil proceedings. It held that Member States must simply ensure that they strike the right balance between competing fundamental rights when applying the national laws which transpose the Directives and that they interpret them in a manner which is consistent with fundamental rights and general principles of Community law.60

Avoiding the question? Issues arising in the aftermath of Promusicae

When it comes to determining how the right to property of IPR holders can be reconciled with the right to data protection of alleged copyright infringers, the Promusicae judgment gives rise to more questions than those asked of the Court initially.

The ECJ’s interpretation of Article 15(1) of the E-Privacy Directive is, at best, questionable.61 Moreover, the judgment reached by the Court runs the risk of leading to forum shopping. It is a necessary consequence of the judgment that the levels of IPR protection and data protection will vary within the European Union depending on how the balance referred to by the Court is struck nationally.62 As Groussot63 highlights “The disparities between the legislation of the Member

60 Para. 68

61 The reference in Article 15(1) of the E-Privacy Directive to Article 13(1) of the Data Protection Directive was interpreted by the Court to mean that all of the Article 13(1) exceptions also apply to the E-Privacy Directive. This interpretation of the provision is not entirely justified on a strict reading of the text, which sets out a list of exceptions and then states “as referred to in Article 13(1)”. In fact, a literal reading of the provision would indicate that the exceptions in Article 15(1) that are identical to those in Article 13(1) should be applied in the same manner rather than that all of the Article 13(1) exceptions should be included within the scope of Article 15(1). Article 13 allows the communication of data to “protect the rights and freedoms of others” and therefore the Court applied this exception to the E-Privacy Directive.

62 Wei has noted this point: “Therefore, in the EU, there is room for Member States to adopt different approaches on whether or not they place privacy rights of individuals at a higher level than intellectual property rights of others” (see Wei, “ISP indirect copyright liability: conflicts of rights on the internet”, [2009] Computer and Telecommunications Law Review 15(8) 181). As has Kuner when he states that “...the ECJ’s judgment may lead to a further fragmentation of the law, in which some Member States allow such use of personal data (ie. Its disclosure for the purposes of pursuing civil infringements) but others do not” (see Kuner, “Data protection and rights protection on the Internet: the Promusicae judgment of the European Court of Justice” (2008) European Intellectual Property Review 30(5) 199).

New Technologies and the Right to Privacy
States as to liability in civil proceedings endanger the coherence of the internal market. It appears clear that the Community legislature and the Court of Justice in *Promusicae* have not provided a magic solution for filling those gaps”.64 This is indeed ironic given that all of the secondary legislation in this field to date has been adopted on the premise of promoting further approximation of the Internal Market. Perhaps most importantly however is the lack of detailed consideration by the ECJ of the fundamental rights issues raised in the case.

*Living up to its “human rights” reputation?*

Balancing the right to data protection against the right to IP is a formidable task and the practical consequences of failing to achieve the right balance between these rights cannot be overemphasized. As Koempel correctly points out, “consumers will only readily take up new digital services if they are reassured that their personal data is sufficiently protected and not abused for marketing purposes or worse”.65 Wei also notes that by revealing the personal identifying data of an individual without their consent there is a risk of misuse, abuse or mistake and of “casting a ‘chill’ on their privacy”.66 Moreover, aside from the need to protect the right to property of IPR holders, copyright protection benefits society as a whole67 as without appropriate legal copyright protection, copyright owners would “lack the incentive to go on being creative and making a living from their work”.68

In light of the European Union’s enhanced commitment to human rights in recent years69 it is clear that the ECJ will need to balance competing rights and interests on a more frequent basis in the future.70 Therefore *Promusicae* provided the ECJ with an opportunity to demonstrate its capacity to provide concrete guidance to Member States on human rights issues. Although given the current legislative framework the final conclusion reached by the Court may be the correct

64 Kuner, supra note 62, also warns that “In the internet age, this kind of national approach is bound to lead to difficulties”.
65 Supra note 1.
66 Supra note 62.
67 Becker (supra note 17) remarks that “..legal protection of the Right to Property against State intervention not only serves the individual owner. It has also a social purpose by encouraging innovation, technical development, and investment”.
68 Ibid.
69 As evidenced by the Charter, the EU’s adherence to the European Convention of Human Rights and the increased dialogue between the ECJ and the European Court of Human Rights (for instance, in cases such as *Bosphorus Hava Yollari Turizm* v. *Ireland*, App. No. 45036/98, 2006 42 EHRRI).
70 This is a point which Groussot has also highlighted (supra note 63).
one, it is arguable that the balance struck by the judgment between the protection of personal data and IPRs is skewed. The judgment has been criticized for dealing a blow to the music industry. As Wei has noted, “Neither the right to privacy, nor copyright, is an absolute right, and in cases of a clash between these two rights, it would not be fair or appropriate to prioritise the privacy right and disregard copyright, as both rights deserve respect and have their economic and individual importance”. Without the personal data of those who infringe copyright, copyright owners cannot effectively protect their rights. The judgment may therefore strike at the very heart of the right to property although it proclaims that this should not be the case when is says that “…the Member States must, when transposing the directives mentioned above, take care to rely on an interpretation of the directives which allows a fair balance to be struck between the various fundamental rights protected by the Community legal order”. Once again however, the Court does not however provide the national Courts with any indication as to how this balance can be struck.

III. Solutions

One positive element some commentators have gleaned from the Promusicae judgment is that it will allow national legislatures to be creative when considering how to balance these rights. Some potential solutions to this balancing problem will therefore now be outlined.

i) Bolstering the role of ISPs in copyright protection

As the sole guardians of the personal data necessary to identify those who infringe copyright, there is increasing pressure put on ISPs by copyright societies to play a role in copyright enforcement. A range of solutions has therefore been mooted proposing varying roles for ISP holders. These solutions will now be set out and their compatibility with data protection law will be considered.

---

72 Kuner (supra note 62) argues that: “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”.
73 This point is emphasised by Coudert and Werkers; See Coudert and Werkers, “In the aftermath of the Promusicae case: how to strike the balance?” (2010) International Journal of Law and Information Technology 18(1) 50.
a) An ISP “warning system”

One of the least intrusive roles an ISP can play in helping to ensure the enforcement of copyright is to notify subscribers to its services, the data subjects, when they infringe copyright. In this case, under certain conditions rights holders could monitor traffic on P2P file-sharing systems and if an infringement is spotted notify the ISP. The ISP would then forward a notice to the user highlighting the conditions of the subscription agreement which bind the user and setting out some of the broader consequences of copyright infringement. This is essentially the solution set out in the UK’s Digital Economy Bill which is currently at Committee stage in the House of Lords. This Bill provides that ISPs shall notify their subscribers if copyright owners have reported infringing activity linked to their IP address. The ISPs then keep track of the number of reports concerning each subscriber and compile an anonymous list of some or all of those who are reported. A Court order is then sought by the IPR holders to obtain the personal details of those concerned so that the IPR holders can initiate proceedings against them.

This solution has the advantage that it does not lead to the disclosure of the personal data of the alleged infringers (or not without the safeguard of a Court order, as in the UK) yet there is a chance that the infringement will cease as a result of the communication sent by the ISP. The problem with the solution however is that it is not guaranteed that the infringement will cease as a result of the ISP’s reminder.

b) “Three strikes” laws

As a result of the perception that the “warning system” does not act as a sufficient deterrent for copyright infringers, a second option which has been mooted goes a step further by providing for sanctions once an alleged infringement has occurred repeatedly. France sought to introduce legislation which would cut off the internet connection of the user once IPRs had allegedly been infringed on three occasions. This law proposed that ISPs would inform a regulatory body (HADOPI) on the “third strike” and that this regulatory body would then axe the alleged infringer’s connection. This proposal (commonly known as “Hadopi”) was rejected by the

---

74 This is the solution preferred by Kuner (supra note 62).
75 See http://www.publications.parliament.uk/pa/ld200910/ldbills/001/2010001.pdf
76 This is presuming that the IP Address itself does not constitute “personal data” within the meaning of the Data Protection Directive. This point is highly contested and the ECJ has yet to pronounce on it (see in this regard, Coudert and Werkers, supra note 73).
National Assembly despite strong government support. It was then accepted by the National Assembly on a second reading and by the Senate and therefore passed into law\textsuperscript{77}. The law was challenged before the French Constitutional Court on the grounds that some of its provisions were unconstitutional. The \textit{Conseil Constitutionnel} held that as a result of the development of the internet and its importance for the participation in democratic life, freedom of expression includes the freedom to access online public communication services. The Court held that the initial powers to sanction individuals by restraining or preventing their access to the internet as subscribers set out in the law were incompatible with this right. According to the Court, this power to sanction could only be exercised by the judiciary. The Court also held that by obliging the internet subscriber to prove that the copyright infringement alleged was undertaken by a third party, the presumption of innocence set out in Article 9 of the Declaration was also violated. As a result of these breaches the Constitutional Court struck down the provisions in the Hadopi law relative to the imposition of sanctions.\textsuperscript{78} It was also argued before the Court that the Hadopi law “produces a patently unbalanced reconciliation between the protection of copyright and the right to privacy” as it introduces a "generalized control of electronic communications" incompatible with the constitutional requirements of the right to privacy.\textsuperscript{79} The Court held that the authorisation given to the administrative authority to collect personal data “cannot, without constituting a disproportionate infringement of the right to privacy, have other purposes than to enable copyright holders to institute legal proceedings on the same footing as any natural or legal entity who has been the victim of an offence”. 

\textsuperscript{77} LOI n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet. See http://legifrance.gouv.fr/affichTexte.do;jsessionid=3669E0FCB4D87ED37C2C3517BF5B6BB5.tpdjo11v_1?cidTexte=LEGITEXT000020736830&dateTexte=20100202
\textsuperscript{78} The Hadopi law may therefore now be compatible with the Telecoms package currently being negotiated by the European Institutions and in particular the “Internet freedom provision” inserted at the insistence of the European Parliament following protracted debate. This provision explicitly states that “....any measures taken by Member States regarding access to or use of services and applications through telecoms networks must respect the fundamental rights and freedoms of citizens, as they are guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and in general principles of EU law”. It also states that such measures “must respect the presumption of innocence and the right to privacy”. When commenting on this provision, Commissioner Reding stated that "The new internet freedom provision represents a great victory for the rights and freedoms of European citizens” and that “‘Three-strikes-laws', which could cut off Internet access without a prior fair and impartial procedure or without effective and timely judicial review, will certainly not become part of European law.”
\textsuperscript{79} Supra note 77, para. 21.
The Digital Economy Bill also provides for further sanctions should the initial obligations on ISPs set out therein prove insufficient to significantly reduce the level of online copyright infringement. In such a case, the Secretary of State may impose further “technical obligations” on ISPs on the basis of a report from OFCOM or on the basis of other relevant considerations. The technical obligations would require ISPs to take measures to limit the internet access of certain subscribers who are allegedly repeat infringers by capping their bandwidth or shaping it in such a way that the subscriber would no longer be able to file-share or even temporarily suspending their broadband connection.

c) The compatibility of increased ISP involvement with European Data Protection Law

It follows from the ECJ’s Promusicae judgment that European Data Protection law does not prohibit Member States from enacting legislation which requires ISPs to provide copyright holders with the personal data of alleged infringers. In principle therefore, legislation such as the Digital Economy Bill and the Hadopi law ought to comply with Data Protection Law and not infringe the right to privacy. It is advocated however that the compatibility of these measures with the right to privacy and European Data Protection law is, at best, uncertain.

First, the Article 29 Working Party has advocated that imposing any duty on an ISP to monitor is contrary to Article 15(1) of the E-Commerce Directive which states that: “Member States shall not impose a general obligation on providers...to monitor the information which they transmit or store, nor a general obligation to seek facts or circumstances indicating illicit activity”. Strangely, this provision was not considered by the Court in Promusicae and therefore the argument of the Working Party may well be a valid one. Moreover, the compatibility of such monitoring with Article 8 ECHR is extremely questionable. Irrespective of doctrinal debates about the outer limits of this notion, the ECtHR has made it clear that Article 8 ECHR certainly encompasses the narrow concept of privacy as freedom from surveillance or prying. In this regard, the ECtHR has held, for instance, that a person has the right not to be filmed by closed

81 Coudert and Werkers (supra note 73) also make this point. They state “It is doubtful whether the preventive measures proposed by copyright societies comply with this principle [of proportionality]. The implementation of filters goes against the prohibition on all large-scale exploratory and general surveillance of telecommunications, and is not compliant with the principle of specificity”.

New Technologies and the Right to Privacy
circuit television (cctv) cameras even in public places. One could conclude from the case of *Amann v. Switzerland* that even mere monitoring of IP address holders and the subsequent registering of their behaviour in itself constitutes a violation of Article 8 ECHR.

Second, even if this initial surveillance is deemed lawful, the subsequent retention of the data which is sought by IPR holders from ISPs may not be compatible with the rights to privacy or data protection. In *Promusicae*, the Court hinted at the fact that this retention might not be lawful but refused to consider the matter by stating “It must therefore be accepted that that communication falls within the scope of Directive 2002/58, although the compliance of the data storage itself with the requirements of that directive is not at issue in the main proceedings”. The Advocate General was more forthright on this point when she noted that “It may be doubted whether the storage of traffic data of all users without any concrete suspicions – laying in a stock, as it were – is compatible with fundamental rights”. However, she proceeds by stating, like the Court, that “Such an interference with fundamental rights would be beyond the scope of these proceedings...” but that “…this question may have to be examined one day in connection with the [Data Retention Directive]”. However, when the validity of the Data Retention Directive was challenged in the case of *Ireland v. Council and Parliament*, the Directive was upheld. However, in that case the Court focused exclusively on the question of whether the Directive was enacted on the correct legal basis with the Court expressly stating that the question it was answering, as formulated in the Irish challenge to the Directive, did not concern the possible breach of fundamental rights as regards the governing of data. As one commentator has remarked “One may perhaps therefore wonder whether such a statement was an invitation to such consideration”. The Article 29 Working Party has also voiced its opposition to such a storage obligation stating that “ISPs can neither be obliged, except in specific cases where there

---

83 The applicant in *Amann* was a salesman who received a business call from a client working at the Soviet embassy in Bern. The call was intercepted by the Swiss Public Prosecutor and an information card on the applicant was later created and stored by the Public Prosecutor. In that case, the Court held that the applicant’s right to private life had been breached by the creation of the card and its storage in the Confederation’s card index despite the fact that the information on it was never disseminated.
84 Para. 45
85 Para. 82
86 Ibid.
is an injunction of enforcement authorities, to provide for a general “a priori” storage of all traffic data related to copyright”. Moreover, such an obligation to store appears to be contrary to Article 8 ECHR as the systematic filing and storage of information, even public information, has been deemed to breach this provision.\textsuperscript{89} Finally, the questionable compatibility of data storage with fundamental rights is still in the limelight following the decision of the German Constitutional Court that the national legislation implementing the Data Retention Directive breaches the constitutional right to privacy.\textsuperscript{90} The possibility therefore remains open to challenge national legislation imposing retention obligations on ISPs on this ground.

In \textit{Promusicae} the ECJ side-stepped these considerations by finding that Member States may provide for exemptions to the confidentiality obligation imposed on ISPs by the E-Privacy Directive when it is necessary for the protection of the rights and freedoms of others. Nevertheless, even if such exemptions are permitted and thus legislation such as the Digital Economy Bill and the Hadopi law are not \textit{a priori} unlawful, the measures must be proportionate; that is they must be suitable to attain their objective and must not go further than is necessary in order to achieve this goal. Moreover, they must not strike at the heart of other fundamental rights. Consequently, such measures must preserve the right to data protection and privacy to the greatest extent possible. Wei suggests that this could be achieved by requiring ISPs to provide internet users with notice when their identities are exposed. However, merely informing the data subject that his data has been revealed does not compensate them sufficiently for the breach. To that end, Wei suggests that “a restriction on copyright owners should also be put in place, so that they must compensate a user if the owner obtains details to identify users whom they suspect of infringement which turns out to be improper, without sufficient evidence, and the release of such information under their request leads to harmful consequences for the user”\textsuperscript{91}. This element could certainly be used to ensure that any kind of disclosure system is not abused by IPR holders and that the right to privacy is given sufficient weight.

\textsuperscript{90} See \url{http://euobserver.com/9/29595/?rk=1} viewed on 5 March 2010.
\textsuperscript{91} Supra note 62
ii) Vicarious liability for third parties to infringement

Another potential option, suggested by Wei\(^92\), is to hold liable those who distribute a product with the clear intent that users will avail of it to engage in direct infringement. This path was taken by the United States Supreme Court in *MGM Studios Inc. v. Grokster Ltd.*\(^93\) In that case the Supreme Court unanimously concurred that Grokster could be held liable for copyright infringement as a result of its P2P file-sharing system. Justice Souster stated on behalf of the Justices that “We hold that one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties.” According to Wei, attaching liability to those who induce copyright infringement does not “[attempt] to ‘chill’ legitimate innovation and deny public access to the information, but it sensibly limits liability to culpable conduct of the inducer in order to strike a proper balance between protecting intellectual property to promote creative activities and the importance of not impeding creative and innovative conduct”. More importantly perhaps is that this solution means that neither the rights of data subjects nor of copyright holders will be infringed and copyright will be protected; the need to balance the right to data protection against the right to property would therefore not arise. Nevertheless, the disadvantages of such a solution are also clear. It enables data subjects to breach copyright safe in the knowledge that it is the intermediary who has provided them with the means to illegally download the copyright protected material that will be prosecuted for the infringement. Such a solution is therefore undesirable from a public policy perspective. Moreover, despite Wei’s assertion to the contrary, there is a risk that by condemning P2P file-sharing systems for third party liability there will be less innovation even when it comes to the creation of legal file-sharing technologies in the future.

IV. Conclusion

This paper set out to address how the right to data protection can be reconciled with the right to property of copyright holders in the context of copyright enforcement under European law. The *Promusicae* judgment considered this question but reached the unsatisfactory conclusion that

\(^{92}\) Ibid.

European Data Protection law neither prohibits nor compels Member States from adopting legislation to oblige ISPs to disclose the personal data of their subscribers thereby passing the “hot potatoe” back to Member States. Legislation imposing such an obligation to disclose on ISPs is therefore increasing in popularity in Member States. Despite the ECJ’s finding that such disclosure is compatible with European Data Protection legislation, it is questionable whether such legislation is compatible with the right to privacy, a general principle of European law. It is advocated that the surveillance and storage of such personal traffic data by ISPs violates the right to privacy of users. In order to justify such legislation, Member States must therefore ensure that their copyright enforcement legislation does not disproportionately interfere with this right. More safeguards will therefore be required before such legislation would pass muster before the ECtHR. Given the Court’s reluctance to provide guidance to Member States on this issue, it is perhaps time for the European legislature to clarify how this balance should be struck. Indeed, this is the conclusion also reached by Leistner94 who notes “The reserved attitude of the Court highlights the need for comprehensive reform and harmonisation of ISPs liability in the Community in the near future”.