URBAN GUERRILLA & PIRACY SURVEILLANCE: ACCIDENTAL CASUALTIES IN FIGHTING PIRACY IN P2P NETWORKS IN EUROPE

GIANCARLO F. FROSIO*

Copyright law is facing its biggest challenge yet as it copes with technological development and an increasingly global information market. The advent of peer-to-peer networks has multiplied the threat to the peaceful enjoyment of copyrights and has made any user a potential infringer. Nonetheless, copyright holders, in targeting those users, have greatly impinged on the users' fundamental rights, in particular the right to privacy.

This Article examines the tension between copyright and privacy in Europe. In particular, this Article will review the legal framework of the debate, as well as the relevant case law, both at the community and national levels. The analysis will specifically focus on the lawfulness of the collection of personal data of peer-to-peer network users as a tool to fight piracy.

In order to strike a fair balance between copyright and privacy, many different subject matters, such as data protection law, copyright law and e-commerce law, must be carefully weighted. In addition, relevant opinions on the issue of fair balance of copyright and privacy have been expressed by the European Data Protection Working Party and the European Court of Justice (ECJ). Finally, since the EU law, when applied to file exchange in peer-to-peer systems is inconclusive, we must turn to national courts and authorities to verify the practical implementation of the ECJ guidelines.

* S.J.D. Candidate, Duke University School of Law, Durham, North Carolina; Assistant Director, WIPO-Turin Master of Laws in Intellectual Property, Turin, Italy. J.D., Università Cattolica del Sacro Cuore, Milan, Italy; LL.M., Strathclyde University, Glasgow, UK; LL.M., Duke University School of Law, Durham, North Carolina.
I. INTRODUCTION

Copyright law faces an unprecedented challenge of regulating technological development in an increasingly global economy. According to John V. Pavlik, "[e]arlier generations of technology . . . have presented challenges to existing copyright law, but none have posed the same threat as the digital age."1

Digitalisation, with its capacity of making perfect copies indistinguishable from the original, digital compression technologies, which permit large media files to be compressed with little loss of quality, and the global and instantaneous Internet

---

powers of propagation, now multiplied by the high bandwidth speed connections, offer a synergy that is almost invincible.

All of these elements are aggregated by the "darknet," the mechanisms and infrastructure for sharing digital content.\(^2\) The darknet constitutes one of the greatest threats to copyright law in the information society.\(^3\) Copying and distributing a large number of high quality digital files with only a home computer and Internet access has become considerably easier with the advent of peer-to-peer file sharing programs that allow users to search for and download files from each others' computers.

Copyright holders are fighting a fierce battle against peer-to-peer systems. The first casualty of this battle was the file sharing software, developed around a centralized architecture.\(^4\) More recently, the distributors of the decentralized peer-to-peer systems have been declared liable for inducing copyright infringement.\(^5\) Nonetheless, the fundamental principle, upheld in 1984 by the U.S. Supreme Court's Betamax decision, that technological devices, capable of substantial non-infringing uses, are lawful,\(^6\) is still valid.\(^7\) In fact, the Grokster decision only rules out software distribution modalities inducing the infringement of copyright.\(^8\) Again, the Dutch Supreme Court reaffirmed the applicability of the Betamax case principle to peer-to-peer software and platform.\(^9\)

---


3. Id. at 158.


7. See Grokster, 545 U.S. at 932-33.

8. Id. at 939-41.

Inevitably, new and judicially unobjectionable peer-to-peer models and architectures, such as BitTorrent,\textsuperscript{10} are ready to substitute the old technology outlawed by the courts.

by the Dutch music rights society BUMA/STEMRA, the Supreme Court of the Netherlands clarified that the providers of the file sharing system Kazaa were not liable for direct copyright infringement nor were they liable for the offering and public distribution of the peer-to-peer software. \textit{Id.} Although under a different legal framework, the Dutch Court reached the opposite conclusion from the U.S. Supreme Court in the Grokster case. \textit{See Grokster, supra} note 5, at 919. At that point, the Dutch decision was the first issued worldwide by a Supreme Court on the legality of peer-to-peer systems. For this reason, Christiaan Alberdingk Thijm, Kazaa’s lawyer, declared that “[t]his is a great ruling . . . [w]hat is important is that this ruling does not only set a precedent in the Netherlands, but also worldwide.” Joris Evers, \textit{Dutch Supreme Court Rules Kazaa Legal}, PCWORLD.COM, Dec. 19, 2003, http://www.pcworld.com/news/article/0,aid,113968,00.asp. But the International Federation of the Phonographic Industry (IFPI) issued a statement calling the Dutch ruling “a flawed judgment” of “minor importance” as it will “almost certainly be overtaken by future decisions based on a full airing of the facts.” \textit{Id.} \textit{See also} Jan Libbenga, \textit{Dutch Supreme Court Rules Kazaa Legal}, THE REGISTER, Dec. 19, 2003, http://www.theregister.co.uk/2003/12/19/dutch_supreme_court_rules_kazaa; Declan McCullagh, \textit{Kazaa is legal! Netherlands Supreme Court says so [ip]}, POLITECH, Dec. 19, 2003, http://seclists.org/lists/politech/2003/Dec/0042.html. \textit{But see} Norwegian Kort om Hoyesterett [Supreme Court] of Jan. 27, 2005, 2004/882 (Norw.), \textit{available at} http://www.lessig.org/blog/archives/Napster-case.pdf (English summary by Georg P. Krog) (regarding the different issue of hyperlinking to infringing material in a case brought by the Tono, Norwegian music industry lobby group, against Frank Allan Bruvik, who set up a website called napster.no back in 2001 that allowed his users to submit direct links to MP3 files). The case is relevant because the Court rejected the argument that linking corresponds with the concept of “mak[ing] available to the public” and convicted the defendant on the grounds of contributory infringement, stating, similarly to the Grokster case, that Bruvik acted willfully. \textit{Id.} Willfulness of the behavior could be inferred from the welcome message on the home page: “Welcome to napster.no. You are now visiting Norway’s largest and best website with music free of charge. Here you may download as much music as you desire.” \textit{Id.} \textit{First Norwegian Verdict on Hyperlink}, EDRI-GRAM, Aug. 10, 2005, http://www.edri.org/edrigram/number3.16/hyperlinks. \textit{See also} Thomas Rieber-Mohn, \textit{The Norwegian Supreme Court Decides the napster.no Case}, IRIS MERLIN, Mar. 29, 2005, http://merlin.obs.ceu.int/iris/2005/3/article29.en.html.

II. PIRACY SURVEILLANCE: DICHOTOMY BETWEEN PRIVACY AND COPYRIGHT ENFORCEMENT

Unable to illegalize file-sharing technologies both in Europe and in the U.S., the music and record industry adopted the strategy to fight unauthorized digital content distribution on the Internet by targeting the users who violate copyright laws through peer-to-peer systems.\textsuperscript{11}

The end-user anti-piracy strategy was initiated in the United States. The Recording Industry Association of America brought more than 9,000 people to court and reached out-of-court settlements with hundreds of these alleged copyright infringers.\textsuperscript{12} The average settlement was approximately $3000, but the association claimed up to $150,000 for every pirated song.\textsuperscript{13} Such harsh action curbed the propensity of six million Americans from downloading copyrighted music from the Internet.\textsuperscript{14}

The copyright owners have been determined to conduct this sort of urban guerrilla warfare also in Europe.\textsuperscript{15} In the recent past, the music industry has started hundreds of lawsuits in Europe, including in the United Kingdom, France, Austria, Denmark, Germany, Italy, Finland, Iceland, Ireland, and the Netherlands.\textsuperscript{16}


\textsuperscript{14} Id.; see Press Release, supra note 12.

\textsuperscript{15} See Yinka Adegoke, Copyright Law Update Could Free Music Industry to Sue, NEW MEDIA AGE, Sept. 18, 2003http://www.nma.co.uk/news/copyright-law-update-could-free-music-industry-to-sue/4832.article (quoting Peter Jamieson, Chairman, British Phonographic Industry; “I don’t want to sue consumers, but when the legal framework is in place we’ll follow due process.”).

The "nicest litigators in the world" have been working endlessly.\textsuperscript{17} Many people have faced sanctions or paid fines in Europe, and IFPI has been dealing with several thousand lawsuits worldwide.\textsuperscript{18}

Much debate surrounded the copyright owners' action plan. Doubts have been raised on the adequacy of such an aggressive approach.\textsuperscript{19} Commenters have questioned its efficiency for the judicial system.\textsuperscript{20} Internet users' and digital content consumers' privacy, "the right to be le[f]t alone – the most comprehensive of rights and the right most valued by civilized men[,]"\textsuperscript{21} has been a


19. \textit{See} COMP. SCI. & TELECOMM. BD. \textit{et al., The Digital Dilemma: Intellectual Property in The Information Age} 310 (2000) ("Some lessons from prohibition in the early 20\textsuperscript{th} century should be remembered: Heavy-handed rhetoric and enforcement practices bred less respect for the law, not more, and left people feeling justified in flouting the law.").


particular concern. The debate revolves around the collection of peer-to-peer system users’ data through various technological devices and the disclosure of users’ identities by Internet Service Providers (ISPs). The dispute has its origins in the U.S. and has only most recently surfaced in Europe.

22. See Sonia K. Katyal, *Privacy vs. Piracy*, 7 YALE J. L. & TECH. 222, 293-304 (2005) (describing the key tools used by the Movie Picture Association of America (MPAA), the Record Industry Association of America (RIAA), and the International Federation of the Phonographic Industry (IFPI) to fight online piracy and distribution of protected content through file-sharing systems are software technologies running the Internet in search of unlawful activities.) The movie studios provide the MPAA software, sometimes referred to as Ranger, with a constantly updated list of films. *Id.* at 294. The software sets out on the Internet looking for those films on web sites, chat rooms, and peer-to-peer sites. *Id.* When a movie title is found, the scanning software marks the location and decides whether the movie infringes on the copyright. *Id.* The software collects the IP addresses of the computers sharing the files and identifies the ISP by a reverse ISP range look up. *Id.* On the basis of the data collected, the MPAA asks the ISPs hosting the site or the user infringing on the copyright to take down the offending films. *Id.* In the case the ISPs do not collaborate, the MPAA may contact local authorities asking them to seize computer servers storing the pirated films. *Id.* On the music side, RIAA and IFPI have begun using *spy bots* that, in the same manner as the MPAA’s software, search shared files for copyrighted works and send instant messages as pop-ups on the screens of users as they are swapping unauthorised copies of songs. *Id.* at 341-42. Another of the latest guerrilla tactics in fighting online copyright infringement is *spoofing*, or replacing music offered on a file-sharing website with hissing noise beyond the first twenty seconds of a song. See *id.* at 297, 357; Nicklaus Lundblad, *Noise Wars: Is the Answer to the Machine in the Noise?*, ST. ANNA RES., INST. (Apr. 15, 2003), http://www.skriver.nu/lundblad_bileta2003.pdf.

23. See In re Verizon Internet Servs., Inc., 240 F. Supp. 2d 24, 44-45 (D.C. Cir. 2003) (granting RIAA’s motion to enforce a subpoena on Verizon under the Digital Millenium Copyright Act because Verizon refused to reveal the identity of its subscriber who allegedly used Kazaa peer-to-peer software to share music online.); In re Verizon Internet Servs., Inc., 257 F. Supp. 2d 244, 275 (D.C. Cir. 2003) (denying Verizon’s motion to quash subpoena); Recording Indus. Ass’n of Am., Inc. v. Verizon Internet Servs., Inc., 351 F.3d 1229, 1231 (D.C. Cir. 2003) (stating the subpoena may only be issued to an ISP which is storing copyright-infringing material on its servers); see also Jonathan Krim, *A Story of Piracy and Privacy*, WASH. POST, Sept. 5, 2002, at E01 (In Apr. 2003, the D.C. District Court upheld the right of the recording industry to reveal the names of the customers suspected of illegally sharing music online); Jonathan Krim, *Recording Firms Win Copyright Ruling*, WASH. POST, Jan. 22, 2003, at E01; David McGuire, *Verizon Challenging Copyright Ruling*, WASHINGTONPOST.COM, Jan. 30, 2003, available at http://www.goliath.ecnex.com/coms2/gi_0198-118854/Verizon-Challenging-
This phenomenon, renamed "piracy surveillance," is a consistent threat to users' privacy. The discovery of spyware-like hiding techniques, Trojan horses and various pieces of malware in Digital Rights Management (DRM) systems are a corroboration in practice of the perceived privacy risks. The installation of malicious software, without any mention in the End-User License Agreement (EULA), indicates how far copyright owners may go in creating "extrajudicial systems of monitoring and enforcement" that prevents infringement by using the code as a tool to influence, modify and regulate behavior. Whether "the answer to the machine is in the machine" is a very disputable conclusion, and the implementation of such a model can lead to abuses and to the

Copyright-Ruling.html; Katyal, infra note 22, at 281-90.


29. Lessig, supra note 21, at 6 ("In cyberspace we must understand how code regulates - how the software and the hardware that make cyberspace what it is regulate cyberspace as it is. As William Mitchell describes it, this code is cyberspace's 'law'. Code is law."); see also WILLIAM J. MITCHELL, THE CITY OF BITS: SPACE, PLACE AND THE INFOBAN 159 (MIT Press, 1995); James Boyle, Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors, 66 U. CIN. L. REV. 177, 190 (1998); ANDREW L. SHAPIRO, THE CONTROL REVOLUTION: HOW THE INTERNET IS PUTTING INDIVIDUALS IN CHARGE AND CHANGING THE WORLD WE KNOW 73-78 (Public Affairs, 1999).

impairment of individual rights.

In addition, any software in search of infringing internet activities is only capable of identifying machines, but not a person performing the unlawful activities.\(^{31}\) This creates extreme uncertainties in the allocation of liability, particularly because of the diffusion of open wireless networks.\(^{32}\) In fact, technological enforcement of copyright necessarily presupposes coincidence between machine and infringer. This could be the harbinger of substantial violations of individual rights, particularly in the pre-judicial phase in which the alleged infringer must be singled out. If criminal penalties are attached to copyright infringement, at least in civil law systems, further concerns exist because technological protection is unresponsive to any principle of personal liability of the criminal conduct. Under most international legal frameworks, criminal liability is strictly personal and nobody can be charged and prosecuted for an offence committed by others. Hence, any mechanisms that allocates criminal liability upon a principle of objective liability, regardless of the fact that the criminal act may

\(^{31}\) See IP Address Alone Insufficient To Identify Pirate Court Rules, TORRENTFREAK (June 15, 2009), http://torrentfreak.com/court-rules-that-ip-address-alone-insufficient-to-identify-infringer-090615/ (reporting that a court in Rome held that "the mere ownership" of an IP address from where an infringement took place is not sufficient to identify an infringer); Guido Scorza, Non Basta Un IP Per Fare Un Pirata, PUNTO INFORMATICO (June 15, 2009), http://punto-informatico.it/2643585/PI/ Comment/non-basta-un-ip-fare-unpirata.aspx (providing further details on the court of Rome decision) (in Italian only).

\(^{32}\) In the case of wireless connection, the average user faces technological difficulties in setting up encryption protection capable of shielding the system from any external intrusion, if any obligation of encrypting and closing the network can be found at all. See Steven Hinkle, The Inaccuracies of Using 'Spy Bots' for Copyright Enforcement, BOYCOTT-RIAA (May 18, 2003, 6:57 AM), http://www.boycott-riaa.com/article/6716. In a Swedish case, where a man has been found guilty of uploading a copyrighted movie on a p2p hub, the alleged infringer's defense counsel made a central argument explaining to the Court the lack of certainty of an IP address used as evidence, the presence of many blocks of flats with unencrypted wireless networks, and the capacity of anyone to exploit another's network. See File Shares Trial Closes In Confusion, THE LOCAL, Oct. 12, 2005, http://www.thelocal.se/article.php?id=2271&date=20051012; Sweden Convicts First File-Share, BBC NEWS, Oct. 25, 2005, http://news.bbc.co.uk/1/hi/technology/4376470.stm.
have been committed by a different person, would also pose serious problems of consistency with the fundamental safeguards that govern criminal liability.

III. COPYRIGHT AND PRIVACY CONFLICT IN EUROPE

At the European level, the legal framework in which the debate is inserted is extremely complex. Many different subject matters such as data protection law, copyright law and e-commerce law are involved. On top of that, relevant opinions on the issue of fairly balancing copyright and privacy have been expressed by the European Data Protection Working Party and the European Court of Justice.33

1. The European Legal Framework

Under the 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms, the right to privacy is legally enforceable. The Convention on Human Rights provides "everyone has the right to respect for his private and family life, his home and his correspondence."34 In addition, the Convention provides that "there shall be no interference by public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country."35 Similarly, the Charter of Fundamental Rights of the European Union includes the right of everyone "to the protection of personal data concerning him or her."36 The Charter also provides


35. Id. art. 8, § 2.

that "Intellectual Property shall be protected."37 Directive 95/46/EC,38 Directive 97/66/EC39 and Directive 02/58/EC40 have established a detailed framework for the collection and processing of personal data. In addition, to allow the transfer of data to the U.S., where no specific regulation meeting the same strict European standard exists, the European Union and the U.S. Department of Commerce have implemented the Safe Harbor Agreement establishing regulations for international data flow.41

Directive 00/31/EC, the e-commerce directive, governs service providers' liability.42 Any service provider supplying mere conduit to its users is not liable for any information transmitted by the users if "the provider does not initiate the transmission," "does not select the receiver of the transmission," and "does not select or modify the information contained in the transmission."43 Directive 00/31 has a DMCA-like liability regime for information hosting. In fact, the service provider is not liable if it "does not have actual knowledge of unlawful activity"44 and "acts expeditiously to remove or to disable access to the information."45 However, unlike the DMCA, no Directive 00/31 does not set forth a procedure for notice and take down orders. Private codes of conduct are the only guidance for ISPs’ decision making.46 This lack of legal standards

37. Id. art. 17, § 2.
43. Id. art. 17(1)(a)(b)(c).
44. Id. art. 19(a)(1).
45. Id. art. 18(b)(v).
46. It is notable that Whereas 29 of the Copyright Enforcement Directive specifically provides the development of Codes of Conduct is a "supplementary

In fact, the Motion Picture Association (MPA) and the International Federation of the Phonographic Industry (IFPI) have asked for strong collaboration by ISPs in Europe and drafted a code of self-regulation, for the film and music sector, demanding the ISPs to:

i. remove references and links to copyright infringing sites and services,
ii. require subscribers to consent to identity disclosure in case of a reasonable complaint from right holders or right holders’ collective societies,
iii. develop prototype instant messages directed toward infringers,
iv. terminate contract for “recidivists,”
v. preserve data and evidence necessary to enforce copyright,
vi. implement filtering technologies to block services “substantially” dedicated to illegal file sharing or downloading, and (concluding with an even more extreme demand than the previous),
vii. enforce terms of service prohibiting subscribers from operating a server or consuming excessive bandwidth when “such consumption is a good indicator of infringing activity.”


However, the European Commission clearly takes the side of the entertainment industry and pushes for strong co-operation between producers and Internet providers. During the Cannes Film Festival in 2005, in discussing online film distribution and the establishment of the online film market in Europe, the Commission highlighted two main points. First, cooperation and increased responsibility of the ISPs are necessary to avoid the broadband industry collapse since “so far the ISPs relied on a free-rider model.” UNI Media, Entm’t & Arts, European Commission Starts Initiative on Films Online, Apr. 28, 2004, http://www.union-network.org/unimei.nsf/0/6D84E36862E
may lead ISPs to provide identification information more easily. Additionally, Directive 00/31 does not allow the member states to impose on the ISPs a systematic obligation of surveillance or monitoring of information transmitted or stored, nor “a general obligation actively to seek facts or circumstances indicating illegal activity.” 47 However, EU member states may establish obligations for ISPs to inform the authorities of alleged illegal activity or “obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their services with whom they have storage agreements.” 48

Furthermore, the Copyright Enforcement Directive also contains relevant provisions. 49 The measures designed to ensure a high level of copyright protection existing for certain EU state members should be made available to all the members. In particular, “this is the case with the right of information, which allows precise information to be obtained on the origin of the infringing goods or services, the distribution channels and the identity of any third parties involved in the infringement.” 50 On the right of information, Directive 04/48 states that:

47. See Directive 00/31, supra note 42, art. 15(1).
48. Id. art. 15(2).
49. See Directive 04/48, supra note 46.
50. Id. § 21.
Member States shall ensure that, in the context of proceedings concerning an infringement of an intellectual property right and in response to a justified and proportionate request of the claimant, the competent judicial authorities may order that information on the origin and distribution networks of the goods or services which infringe an intellectual property right be provided by the infringer and/or any other person who: ... (c) was found to be providing on a commercial scale services used in infringing activities.\textsuperscript{51}

Additionally, Directive 04/48 includes a provision that the information ordered will "include the names and addresses of the producers, manufacturers, distributors, suppliers," wholesalers, and retailers of the goods or services and "information on quantities and prices of goods or services."\textsuperscript{52} The provision grants intellectual property holders overbroad subpoena powers to obtain personal information on consumers. The right of information can be directed to ISPs, universities, telecommunications companies and all of the intermediaries involved in an alleged infringement. Judicial authorities would be required to issue orders of disclosure on personal identities and information related to services and goods on the basis of mere allegation of infringement. Therefore, the accused party shall not enjoy the most basic guarantee of fair trial before its identity is disclosed. In fact, in order to evaluate the justification and proportionality of the claimant’s request, judicial authorities have to investigate and find prima facie evidence of infringement without the accused party having any opportunity to be heard and to defend itself at trial. The described mechanism appears to be in violation of Article 6 of the European Convention on Human Rights.\textsuperscript{53}

Directive 04/48 also empowers judicial authorities to issue an interlocutory injunction against intermediaries whose services are used to infringe on intellectual property rights by a third party, to prevent any imminent infringement.\textsuperscript{54} In the case of copyright

\textsuperscript{51} ld. art. 8(1) (emphasis added).
\textsuperscript{52} ld. art. 8(2).
\textsuperscript{53} See EU HR Convention, supra note 34, art. 6.
\textsuperscript{54} ld. art. 9(1)(a).
infringement, cross reference must be made to Directive 01/29/EC stating, under its section on Sanctions and Remedies, that "[m]ember States shall ensure that right holders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right." But, this provision appears inconsistent with the aforementioned service providers’ liability regime detailed in Directive 00/31.

2. The EU Data Protection Working Party

The EU Data Protection Working Party has repeatedly expressed its view on this chaotic legal framework. Toward answering the many concerns surrounding access to personal data of alleged infringers, the EU Data Protection Working Party seriously questions the use of identifiers for the purpose of tracing ‘a priori’ every user, in order to go back to a specific individual in case of a suspected copyright abuse. The tagging of a document should not be linked to an individual except if this link is necessary for the performance of the service or if the individual has been informed and has consented to it.

The Article 29 Working Party has in 2007, and again in 2008, expressly declared that IP addresses do in fact constitute “data relating to an identifiable person” under the EU Data Protection Directive. Further, Article 29 Working Party has stated that

55. Council Directive 01/29, art. 8(3), 2001 O.J. (L 167) 10, 18 (EC) [hereinafter Directive 01/29]. The concept is restated in “whereas” clause 59 of Directive 01/29: [i]n the digital environment, in particular, the services of intermediaries may increasingly be used by third parties for infringing activities. In many cases such intermediaries are best placed to bring such infringing activities to an end. Therefore, without prejudice to any other sanctions and remedies available, right holders should have the possibility of applying for an injunction against an intermediary who carries a third party’s infringement of a protected work or other subject-matter in a network.

Id.


“Internet access providers and managers of local area networks can, using reasonable means, identify Internet users to whom they have attributed IP addresses as they normally systematically ‘log’ in a file the date, time, duration and dynamic IP address given to the Internet user.”

With regard to the processing of IP addresses carried out with the purpose of identifying the users of the computer, as in the case of copyright holders monitoring infringing behaviors, the Working Party is of the opinion that the controller anticipates that the “means likely reasonably to be used” to identify the persons can potentially be made available (e.g., through the courts appealed to - otherwise the collection of the information makes no sense), and therefore the information should be considered personal data.

Coming to the alleged ISPs’ obligation to disclose users’ identities, the Data Protection Working Party points out that “ISPs can neither be obliged, except in specific cases where there is an injunction of enforcement authorities, to provide for a general ‘a priori’ storage of all traffic data related to copyright.” This point has been stressed by the Internet intermediaries as well. In fact, the ISPs are not policing services and the implementation of filtering or blocking technologies is “a slippery slope that can easily lead to a situation we know from China, where all traffic is filtered on the backbone.” The attempt to protect intellectual property rights in

Opinion 2008, supra note 33, at 8.


61. WIPO Seminar on ISP Liability, DRIE (Apr. 20, 2005), http://www.edri.org/edrigram/number3.8/WIPO (At the WIPO Seminar on ISPs’ liability, Verizon Vice President Sarah Deutsch, addressing the MPAA’s proposed ISP code of conduct, made clear that an ISP is not a policing service and called for the respect of users’ privacy rights. Verizon representative added that the implementation of filtering or blocking of technologies, as demanded by the entertainment industry, is “a slippery slope that can easily lead to situations we know from China, where all traffic is filtered on the backbone.”).
the digital environment may lead to a manipulation of the Internet architecture through DRM systems, monitoring and anti-copying measures, to the end of erasing any right to anonymity or privacy.

3. The European Court of Justice: The *Promusicae* Case AND THE *LSG* Case

Recently, the European Court of Justice (ECJ) reviewed the matter of privacy rights of alleged copyright infringers in the *Promusicae* v. *Telefónica de España* 62 and the *LSG* v. *Tele2* decisions.63 The judgments are also relevant as an attempt to coordinate the fragmented and confused communitarian legal framework on point. Both cases make large reference to some of the conclusions of the Lindqvist case, previously decided by the ECJ, where privacy rights were balanced against freedom of expression.64

The *Promusicae* decision, issued by the Grand Chamber of the ECJ, follows Productores de Música de España’s (*Promusicae’s*) request for *Telefónica de España* (Telefónica) to disclose personal information of individuals who allegedly illegally shared


copyrighted files online. Telefónica appealed an order from the Juzgado de lo Mercantil No. 5 de Madrid to disclose this information by arguing that, under relevant Spanish law, Telefónica was obligated to provide the data "only in a criminal investigation or for the purpose of safeguarding public security and national defen[s]e," not in the context of civil proceedings.

Promusicae counter-argued that the specific Spanish law must be applied according to Directives 00/31, 01/29, and 04/48, which prohibit Member States to dismiss, in the aforementioned fashion, the duty to provide the information in question. Therefore, the Juzgado de lo Mercantil No. 5 de Madrid referred the ECJ to rule on the following:

Does Community law, specifically Articles 15(2) and 18 of Directive [2000/31], Articles 8(1) and (2) of Directive [2001/29], Article 8 of Directive [2004/48] and Articles 17(2) and 47 of the Charter . . . permit Member States to limit to the context of a criminal investigation or to safeguard public security and national defence, thus excluding civil proceedings, the duty of operators of electronic communications networks and services, providers of access to telecommunications networks and providers of data storage services to retain and make available connection and traffic data generated by the communications established during the supply of an information society service?

To reach its conclusion, the ECJ carried out a preliminary analysis of the principles included in the EU legislation by stating that Directive 02/58 does not prevent Member States from being obligated to communicate personal data for civil proceedings. Conversely, Art. 15 (1) of Directive 02/58 does not compel EU members to make this obligation either. The ECJ also stated that

68. Id. § 33.
69. Id. § 34.
70. Id. § 54. See Directive 02/58, supra note 39.
71. Promusicae, ECJ No. C-275/06, supra note 62, § 55; see Directive 02/58, supra note 40.
neither Directive 00/31, 01/29, nor 04/48 require EU members to disclose personal data to protect copyrights.\textsuperscript{72} In fact, those directives clarify that effective copyright protection cannot affect the requirements of the protection of personal data.\textsuperscript{73} Finally, the ECJ reviewed the provisions of the EU Charter and examined the balance between the right to a private life, as set out by Articles 7 and 8 of the Charter, and the rights to property protection and an effective remedy, as set out by Articles 17 and 47 of the Charter.\textsuperscript{74} Therefore the ECJ held that EU Member States must apply interpretations of directives that allow for a reasonable balance of community fundamental rights.\textsuperscript{75} Furthermore, the authorities and courts of the Member States must make sure not to depend on interpretations that may conflict with Community law.\textsuperscript{76}

The ECJ, moving from this preliminary consideration, concluded:

the answer to the national court’s initial question must be that Directives 2000/31, 2001/29, 2004/48 and 2002/58 do not require the Member States to lay down, in a situation such as that in the main proceedings, an obligation to communicate personal data in order to ensure effective protection of copyright in the context of civil proceedings. However, Community law requires that, when transposing those directives, the Member States take care to rely on an interpretation of them which allows a fair balance to be struck between the various fundamental rights protected by the Community legal order. Further, when implementing the measures transposing those directives, the authorities and courts of the Member States must not only interpret their national law in a manner consistent with those directives but also make sure that they do not rely on an interpretation of them which would be in conflict with those fundamental rights or with the other

\textsuperscript{72} Promusicae, ECJ No. C-275/06, supra note 62, §§ 57-59.

\textsuperscript{73} See Directive 00/31, supra note 42, art. 1(5) (b) (stating that Directive 00/31 does not apply to Directives 95/46 and 97/66 regarding personal data); Directive 01/29, supra note 55, art. 9; Directive 04/48, supra note 46, art. 8(3)(e).

\textsuperscript{74} Promusicae, ECJ No. C-275/06, supra note 62, § 65; see also EU Charter, supra note 36, art. 7, 8, 17, 47.

\textsuperscript{75} Promusicae, ECJ No. C-275/06, supra note 62, § 70.

\textsuperscript{76} Id.
general principles of Community law, such as the principle of proportionality.\textsuperscript{77}

This decision is not completely satisfactory. Although caution is understandable due to the delicacy of the matter, the ECJ should have given a definite conclusion. The final decision regarding the fair balance between privacy and intellectual property rights remains with national authorities, therefore jeopardizing the consistent application of the European regulatory framework.\textsuperscript{78} It would have been desirable if the ECJ identified all of the relevant criteria to apply the principle of proportionality to the specific case of peer-to-peer data exchange, to the extreme situations where neither privacy nor intellectual property rights should have been sacrificed, and then to strike the fair balance in standard situations.\textsuperscript{79} Absent from this road map, national authorities must strike a balance between the fundamental rights at stake. In doing so, they must be cognizant of the fact that both privacy and intellectual property rights are constitutionally based on equal dignity, therefore an interpretation of the privacy rules that favor intellectual property over privacy would be as unlawful as an interpretation that gives priority to privacy over intellectual property.\textsuperscript{80}

Most recently, on February 19, 2009, the European Court of Justice handed over a second decision on the same subject. The Supreme Court of Austria referred a case between a performing rights organization called LSG and the Austrian ISP Tele2 to the ECJ for a preliminary ruling on the following questions:

\textsuperscript{77} Id.

\textsuperscript{78} Id. at § 67 ("As to those directives [Directive 2000/31, 2001/29, 2004/48, and 2005/58], their provisions are relatively general, since they have to be applied to a large number of different situations which may arise in any of the Member States. They therefore logically include rules which leave the Member States with the necessary discretion to define transposition measures which may be adapted to the various situations possible……,").

\textsuperscript{79} See Davide Sarti, Privacy E Proprietà Intellettuale: La Corte Di Giustizia In Mezzo Al Guado, Nota A Corte CE, 1190 ANNALI ITALIANI DI DIRITTO D’AUTORE (AIDA) 444 (2008) (arguing that the situation under review in the Promusicae case was one of those extreme situations where intellectual property rights should not have been sacrificed).

\textsuperscript{80} Id. at 440.
(1) Is the term "intermediary" in Article 5(1)(a) and Article 8(3) of Directive [2001/29] to be interpreted as including an access provider who merely provides a user with access to the network by allocating him a dynamic IP address but does not himself provide him with any services such as email, FTP or file-sharing services and does not exercise any control, whether de jure or de facto, over the services which the user makes use of?

(2) If the first question is answered in the affirmative:

Is Article 8(3) of Directive [2004/48], with regards to Article 6 and Article 15 of Directive [2002/58], to be interpreted (strictly) as not permitting the disclosure of personal traffic data to private third parties for the purposes of civil proceedings for alleged infringements of exclusive rights protected by copyright (rights of exploitation and use)?

The ECJ delivered a reasoned order, not a judgment, largely referring to the Promusicae case. In response to the first question, the Court clarified that access providers "must be regarded as 'intermediaries' within the meaning of Article 8(3) of Directive 2001/29." That conclusion is grounded on three reasons. Firstly, the Promusicae decision did not rule out the possibility that access providers may be placed under a duty of disclosure pursuant to Article 8(1) of Directive 04/48 by holding that Community law does not impose on the communication of personal data to protect copyright in the context of civil proceedings. Secondly, according to Article 8(3) of Directive 01/29, right holders are entitled "to

81. LSG, Case C-557/07, supra note 63, § 22; see also Oberster Gerichtshof [OGH] [Supreme Court] Feb. 19, 2001, No. C-557/07, ENTScheidungen des ÖSTERREICHISCHEN Obersten GerichtshOFES in ZIVILSACHEN [SZ] (Austria).

82. See PAUL P. CRAIG & GRÁINNE DE BURCA, EU LAW: TEXT, CASES, AND MATERIALS 474 (Oxford University Press 2007) ("Article 104(3) of the Rules of Procedure . . . allows the ECJ to give decision by reasoned order referring to a previous decision or earlier case law, where a question referred is identical to one that has already been answered or where the answer to a question can be clearly deduced from prior case law") (citing Rules of Procedure of the Court of Justice, 1 Dec. 2005, available at www.curia.europa.eu/en/instit/txtdocfr/index.htm).


84. Id. § 41.
apply for an injunction against intermediaries whose services are used by a third party to infringe [on] a copyright or related right. Therefore, access providers must be construed as intermediaries within the meaning of Article 8 (3) of Directive 01/29 because those access providers supply the user with a service capable of being used by a third party to infringe on a copyright and make it possible for unauthorised material to be transmitted between a subscriber to that service and a third party. Finally, the protection sought by Article 8(1) of Directive 01/29 would be substantially diminished if the term ‘intermediaries’ were not covering access providers, who are in possession of the data to identify the users who have infringed on the rights protected by the directive.

The answer to the second question is then fully inferred from the Promusicae decision. National agencies and courts may rely not only on the consistency of community directives but must also interpret the national law to ensure that the interpretation strikes a fair balance between the various fundamental rights and does not conflict with the general community principles, notably the principle of proportionality. The ECJ seems to have failed yet again to explain under which circumstances privacy rights would prevail over the intermediary’s duty of disclosure, and the national bodies provide very little guidance. In reality, the argument used by the Court to come to the conclusion that access providers must be regarded as intermediaries may shed a light on the inner feelings of the ECJ. By saying that access providers are intermediaries within the meaning of Article 8 (3) of Directive 01/29 and noting that the Promusicae decision does not rule out a duty of disclosure of the access providers, the ECJ appears to be of the opinion that disclosure is mandated by a coordinated reading of the relevant directives not to undermine their scope of protection but, that fair balance between fundamental rights may override that reading.

85. Id. § 42.
86. Id. §§ 43-44.
87. Id. § 45.
88. Id. §§ 25-29.
IV. JUDICIAL AND REGULATORY TRENDS IN EU JURISDICTIONS

Overall, the very specific question referred to the ECJ by the Court of Madrid and the Austrian Supreme Court does not find a clear cut answer by applying the EU law principles to the debated issue of file exchange in peer-to-peer systems. Therefore, we must turn to national courts and authorities to verify the practical implementation of the call for fair balance between privacy and intellectual property rights sought by the ECJ.89

1. Germany

Courts in Germany appear consistent in enforcing users' privacy rights.90 German courts seem to favor the opinion that dynamic IP-codes are considered personal data.91 However, this topic has been disputed in Germany during the last few years. Many state data protection authorities and a large part of the legal literature shared the view of the judicial power.92 As such, the processing and


91. Id. (ordering the Federal Ministry of Justice to stop collecting and storing the IP addresses of users of its website without their consent); Landgericht Berlin [LG] [Trial Court of Berlin], Sept. 6, 2007, 23 S 3/07 (F.R.G.) (confirming the previous ruling of the administrative court) See also Verwaltungsgericht Wiesbaden, supra note 90 (considering dynamic IP addresses, as personal data, to be particularly worthy of protection). But see Amtsgericht München [AG] [District Court of Munich], Sept. 30, 2008, 133 C 5677/08 (F.R.G.) (stating that when stored by an internet publisher to keep track of activity on a web page, IP addresses are not personal data under the German Privacy Act because the information cannot be easily used to determine a person’s identity); see also German Court Says ISPs Do Not Violate The Law By Storing IP Addresses, EDRI-GRAM, No. 6.20, Oct. 22, 2008, http://www.edri.org/edri-gram/number6.20/ip-addresses-munchen-court (“However, we should not overestimate the relevance of this decision. It was taken by a local court with no IT experts and the judge did not discuss the dissenting decisions from higher level Berlin courts”).

92. See Maija Palmer, EU Targets Online Privacy Fears, FIN. TIMES, Feb. 11,
collection of IP codes should require consent and notification of the
data subject similar to other personal data.

In Germany, it is still heavily debated whether the copyright
owner should receive a right to disclosure from the access
providers based on judicial authority.\textsuperscript{93} However, three 2005
decisions in the Higher Regional Courts of Munich,\textsuperscript{94} Frankfurt-on-
the-Main,\textsuperscript{95} and Hamburg\textsuperscript{96} courts, quashed earlier verdicts, stating
there is no legal basis for forcing ISPs to provide customers’ data to
the record industry under suspicion of illegal copying. These
decisions follow several identical actions brought simultaneously

\begin{flushleft}
2008, available at http://www.ft.com/cms/s/0/8e98263a-d844-11dc-98f7-
0000779d2ac.html?nelick_check=1 (Peter Schaar, Germany’s Federal Data
Protection Commissioner and chair of the EU Article 29 Working Party, stated “IP
addresses - the unique identifier for a computer on the internet - would be
considered personal information by European regulators and must be handled in
accordance with privacy laws.”); see also Peter Schaar Against Direct Access to
Internet User Data by the Music and Film Industry - Statement at the Hearing of
the Legal Committee, THE FED. COMM’R FOR DATA PROTECTION & FREEDOM OF
INFO. (June 25, 2007), available at
http://www.bfdi.bund.de/kln_118/EN/PublicRelations/PressReleases/2007/23-07-
MusicAndFilm.html (Peter Schaar declared, “[a]ny information about the fact who
has surfe[d] the Internet under which IP-address is subject to the confidentiality of
telecommunications . . . it is only admissible to disclose Internet traffic data if
violations of copy right have been committed to a commercial extent. It would be
completely disproportionate to disclose also the data of sporadic peer-to-peer file-
sharing services . . . .”).
\end{flushleft}

93. See infra notes 94-120.

94. Oberlandesgericht München [OLG] [Higher Regional Court of Munich],
Nov. 2005, 6 U 4696/04 (F.R.G.); see also R. W. Smith, Legal Setback for Music

95. Oberlandesgericht Frankfurt am Main [OLG] [Higher Regional Court of
http://www.auffrecht.de/3792.html; see also Craig Morris, Providers do not Have
to Reveal the Identity of Music Copier, HEISE ONLINE, Jan. 25, 2005, available at
http://www.cebit.de/newsanzeige_e?news=13439&tag=1106694001&source=/ne
wsanzeige_e&noindex.

96. Hanseatisches Oberlandesgericht [OLG] [Higher Regional Court of
http://www.jurpc.de/rechtspt/20050062.htm; see also R. W. Smith, Record Labels
Have no Legal Right to Demand Customer Data from Providers, HEISE ONLINE,
by BMG, Universal Music and EMI to obtain consumer data associated with dynamic IP addresses. The key issue in the debate is the German Copyright Act’s disposition, which provides a right of information against third persons with regards to the origin and distribution of copyright infringing material and requires the disclosure of the infringer’s name and address. The previously mentioned decisions upheld that the obligation applies only to those parties that are involved in illegal activities. The mere action of providing access does not imply any such participation and, hence, no obligation to disclose information applies. The Court rejected any argument related to ISP’s contributory liability because no active role or obligation to monitor the traffic preventively can be placed on the ISP. The courts also denied any liability under the provision of the Teleservices Act, enjoining access providers from “remov[ing] and block[ing]” illegal content because such an obligation does not imply that information must be divulged.

In 2008, the German Federal Constitutional Court ruled that an ISP could only give out IP address information in a serious criminal investigation. In a constitutional complaint against the

---

99. See supra notes 94-96.
100. See Oberlandesgericht, supra note 94; Oberlandesgericht, supra note 95; Hanseatisches, supra note 96.
101. On the ground of accountability as a so-called “Mitstörer” (i.e., co-conspirator or facilitator).
102. See Oberlandesgericht, supra note 94; Oberlandesgericht, supra note 95; Hanseatisches, supra note 96.
German Law on Data Retention, the Court decided that ISPs could store data but severely restricted the use of stored data.\textsuperscript{105} Thus, the Court permitted criminal prosecution authorities to access the data with the permission of a judge, but more importantly, it limited data access to use in the prosecution of severe criminal offenses.\textsuperscript{106} These severe offenses include murder, homicide, tax fraud, economic subsidy fraud, and falsification of documents.\textsuperscript{107} The list restricts using stored data for many types of crimes.\textsuperscript{108} Therefore, by excluding copyright infringement from this extensive list, the Court determined that it did not qualify as a serious criminal offense.\textsuperscript{109}

Prompted by the May 21, 2008 Federal Constitutional Court ruling, the Frankenthal District Court decided that revealing the name and address of a defendant who had been criminally charged with sharing a video game on a file sharing network violated his constitutional right to privacy.\textsuperscript{110} The lawsuit was based on evidence obtained by the Swiss anti-piracy outlet LogiSTEP, which provided copyright holders with the IP address of the defendant.\textsuperscript{111} The copyright holders then used the IP address to start a criminal complaint.\textsuperscript{112} Then, prosecutors requested the name of the defendant from a major German ISP and shared it with the right holders, who subsequently initiated a civil lawsuit against the
defendant.\textsuperscript{113} The court ruled that the ISP was not permitted to give out the defendant’s name because file sharing did not qualify as a serious criminal offense.\textsuperscript{114} Therefore, the disclosure violated the defendant’s constitutional right to privacy.\textsuperscript{115} This decision eliminated the widely used and controversial practice by German right holders of using information obtained from criminal proceedings to start civil proceedings.\textsuperscript{116}

As a partial response to the German Constitutional Court decision, the German Parliament approved a new law forcing ISPs to reveal the identity of alleged infringers who violate copyrights on a commercial scale.\textsuperscript{117} Although this measure removes privacy safeguards for some suspected infringers, it is still debatable whether the new law is a win for the industry or for file-sharers. First, the fine for each copyright violation was significantly reduced from 1000 or more Euros to a maximum of 100 Euros per violation.\textsuperscript{118} In addition, the industry bears all of the legal costs.\textsuperscript{119} Thus, the court’s interpretation of the term “commercial level” shall be very relevant in determining where the balance between privacy rights and copyrights is set.\textsuperscript{120}

2. Austria

Recently, Austrian judicial power has reversed a trend forcing ISPs to disclose personal data of alleged infringers. After a four-year battle, the Austrian Supreme Court decided that ISPs do not have to disclose their customer’s confidential data to copyright owners without the permission of a court.\textsuperscript{121}

\textsuperscript{113} \textit{id.}
\textsuperscript{114} \textit{id.}
\textsuperscript{115} \textit{id.}
\textsuperscript{116} See Luetge, supra note 104, at 2.
\textsuperscript{118} \textit{id.}
\textsuperscript{119} \textit{id.}
\textsuperscript{120} \textit{id.}
\textsuperscript{121} Oberster Gerichtshof [OGH] [Supreme Court] July 14, 2009, No. 4 Ob 41/09x (Austria), available at
Previously, in a case involving an alleged infringer charged with offering several thousand music files for download, the Council Chamber overruled the District Criminal Court of Wien, which had granted the right of disclosure.\textsuperscript{122} The Council Chamber's rejection of the plaintiff's demand was based on the argument that a dynamic IP address is not master data (unlike names, addresses, etc.), but traffic data.\textsuperscript{123} Under Austrian telecommunication law, traffic data enjoys special protection.\textsuperscript{124} Traffic data disclosure is only granted to solve intentional crimes punishable by more than one year in prison.\textsuperscript{125} The decision thus excludes any non-commercial uploading of files punished under Austrian copyright law since the maximum punishment is six months in prison.\textsuperscript{126} Nonetheless, the Court of Appeals reversed the Council Chamber by considering IP addresses equivalent to telephone numbers, and therefore master data.\textsuperscript{127} Since master data is subject only to data protection, telecommunication privacy law restrictions no longer applied. Furthermore, the Court of Appeals ordered the disclosure by enforcing Section 18, paragraph 4 of the E-Commerce Statute, which ordered ISPs to divulge master data "if a third party has a material interest in determining the user's identity to provide evidence of an illegal action."\textsuperscript{128}


\textsuperscript{123} Id.

\textsuperscript{124} Telekommunikationsgesetz [TKG] [Telecommunications Act] Bundesgesetzblatt I [BGBl. I] No. 70/2003, § 99 ¶ 1 (Austria) ("Traffic data may not be stored except in the cases regulated by law and must be immediately deleted or made anonymous by the operator after the end of the connection.") (Author's translation from German to English).


\textsuperscript{126} Urheberrechtsgesetz [UrhG] [Copyright Act], Bundesgesetzblatt I [BGBI I] No. 111/1936, as amended, § 91 (Austria).

\textsuperscript{127} See Oberlandesgerich Wien [OLG] [Court of Appeal of Vienna], Mar. 30, 2005, docket No. 17 B 76/05h, available at http://www.i4j.at/entscheidungen/olgw_76_05h.htm (Austria).

\textsuperscript{128} E-Commerce Gesetz [ECG] [E-Commerce Statute], Bundesgesetzblatt I [BGBl. I] No. 152/2001, § 18 ¶ 4 (Austria) (Author's translation from German to
However, the Austrian Supreme Court denied the right of disclosure, presumably striking a fatal blow to the right holders’ expectations. In the litigation between the performing rights organization LSG and the Austrian ISP Tele2, the service provider turned down LSG’s request of disclosure by claiming the secrecy of the communications. The Court of First Instance and the Court of Appeals upheld the claim of the right holders, and noted the right of access is explicitly provided in the Austrian Copyright Act. After being presented with the case, the Supreme Court suspended the proceeding to obtain a preliminary ruling by the European Court of Justice over whether Directive 02/58 allowed the communication of personal traffic data to the right holders. As described earlier, the ECJ decision largely referred to the Promusicae case and failed once again to explain when privacy rights would prevail over the intermediary’s duty of disclosure. Since access providers are considered intermediaries by the ECJ ruling, the Austrian Supreme Court seemed compelled to decide in favour of the rights holders as Section 87b (3) of the Austrian Copyright Act is unambiguous in granting them right of access. Unexpectedly, the Court decided to classify dynamic IP addresses as traffic data which revived the relevancy of Section 99 of the Telecommunications Act. This made it illegal for internet service


130. See Handelsgerichts Wien [HG] [Commercial Court of Vienna] June 21, 2006, docket No. 18 Cg 67/05z (Austria); Oberlandesgericht Wien [OLG] [Court of Appeal of Vienna] Apr. 12, 2007, docket No. 5 R 193/06y, [OLG Wien] No. 26 (Austria).

131. See Urheberrechtsgesetz § 87b (3) (Austria) (providing that “[i]ntermediaries within the meaning of Paragraph 81(1a) shall give the person whose rights have been infringed upon information as to the identity of the infringer (name and address) or the information necessary to identify the infringer, following an application in writing by the person whose rights have been infringed upon, such application to include sufficient reasons . . . .”) (author’s translation from German to English).

132. See OGH C-557/07, supra note 129.

133. See Axel Anderl, Austria, Update and Trends in COPYRIGHT 2010 (Stuart Sinder, Jonathan Reichman and James Rosini eds., 2009).
providers to store traffic data and required the data to be immediately deleted or made anonymous at the end of the connection. The Court held that

under the current legal framework the information sought could be granted only on the basis of an unlawful processing of traffic data. Since the defendant cannot be bound to any unlawful behaviour, the result of this review is the claim to be dismissed. In general, the enforcement of a claim under § 87b (3) of the Copyright Act may fail because the desired information could be issued only after an unlawful processing of traffic data.

Under Austrian law, it would be illegal to hold on to the information that matches an IP address with a customer.

3. Switzerland

In Switzerland, the activity of the anti-piracy tracking outfit Logistep has come under review. To uncover Internet pirates, Logistep searches for the Internet protocol addresses of people who make music files or videos freely available on the web. Logistep then sends this data to the rights holders, who then file complaints. The Swiss Regulatory Authority and Judiciary have taken two opposing positions on Logistep’s activity. Initially, in January 2008, the Swiss Federal Data Protection and Information Commissioner (FDPIC) issued a decision to have Logistep desist from any further data processing in the absence of legal basis. The Swiss Authority noted that Logistep’s collection of personal data used to search for illegal activity must comply with data protection laws. According to the FDPIC Commissioner, the use

---

134. See Oberster Gerichtshof [OGH] [Supreme Court] July 14, 2009, docket No. 4 Ob 41/09x §§5.3.3, 5.4 (Austria).
135. Id. § 8.
136. Id.
138. Id.
of programs to search and store evidence of copyright infringement on the Internet did not comply with data protection laws because the software undertook permanent surveillance of the Internet and peer-to-peer networks.¹³９ Thus, the Commissioner concluded that this type of investigation should be conducted by law enforcement agencies and not by private parties.

Subsequently, the Federal Administrative Court overruled the decision of the FDPIG.¹⁴⁰ The judges admitted that the data collection by Logistep raised some issues when the individuals were unaware the information was collected.¹⁴¹ However, the court felt Logistep’s activity was the only effective way to fight against Internet piracy, and in the opinion of the court, the end justified the means.¹⁴² Since there are few other ways to fight against this form of piracy, the court considered it unacceptable to allow infringers to avoid legal action by upholding their privacy concerns.¹⁴³ Moreover, the public interest in fighting piracy outweighs the private interest of users to protect their data.¹⁴⁴ Finally, the Court noted it was not essential for Logistep to have an explicit legal basis to operate since they act in a purely private sphere.¹⁴⁵

However, on September 8, 2010, the previous decision hindering users’ personal privacy was overruled by the Swiss Federal Supreme Court. The Supreme Court held that collecting dynamic IP addresses of users allegedly uploading copyright protected works in order to forward those addresses to copyright holders is an unlawful and unjustifiable privacy breach.¹⁴⁶ The Swiss Supreme Court...
Court jurisprudence is now perfectly in line with the position earlier held by the Austrian Supreme Court.

4. The Peppermint Record Case in Italy

A number of recently decided cases raised the issue of the conflict between copyright and privacy in Italy.\(^{147}\) Initially, some Italian citizens received a letter from a small German record label, Peppermint Jam Records.\(^{148}\) Peppermint Records urged recipients of the letter to pay money damages for their use of copyrighted music files shared on peer-to-peer applications.\(^{149}\) Previously, Peppermint Records appointed the Swiss company Logistep AG to collect data related to Internet users allegedly sharing copyrighted files.\(^{150}\) User data, such as connection date and time, IP address, name, hash value, dimensions of the shared file, “guid” code, and user nickname were collected with the help of specific scanning software.\(^{151}\) The software was also capable of determining the dynamic IP addresses, the time the files were offered for download/upload, which files were downloaded/uploaded, and the length of time it took for the files to be copied.\(^{152}\)

Following the work by Logistep, Peppermint Records filed two lawsuits in the Tribunal of Rome against Telecom Italia and Wind Telecommunications, two Italian telecommunication operators and ISPs.\(^{153}\) Each lawsuit sought to obtain disclosure of the names of users whose dynamic IP addresses were identified by Logistep


149. Id.

150. Id.


152. Id.

Initially, two Court orders upheld the right of Peppermint Records to obtain the names of the users and, accordingly, issued an order of disclosure against Telecom Italia and Wind Telecommunications. The orders confirmed that the data collection was acceptable and legitimate in light of the fact that p2p users accept that their IP address will be disclosed to other users of the same program. In addition, the orders asserted that the data protection law cannot be construed as an impediment to the disclosure of the data of alleged infringers. This conclusion was grounded in the Italian Privacy Code, which allows for the processing of personal data without the consent of the person who is subject to the data collection, if processing is necessary to establish or defend a legal claim.

Taking into account the possible repercussions of the privacy law and the court orders mentioned above, the Italian Data Protection Authority (Garante) decided to join in the proceedings before the Tribunal of Rome. The Garante pointed out that the treatment of personal data collected without the data subject’s consent was to be limited to criminal investigations carried out only by public authorities in charge of the protection of national security and defence. Any other solution would be in contrast with the fundamental rights of privacy and secrecy of communications as set out in the constitutional principles,
Community law, and European Convention of Human Rights.\(^{161}\) The Garante further highlighted that the “compression of the [data protection and communications] rights at stake might be proportional only in exchange for the protection of superior values protected by criminal law.”\(^{162}\) As a consequence, the precautionary action of Peppermint Records was rejected because it was aimed at the protection of “inferior values” when compared to the right of secrecy of communications.\(^{163}\) In addition, the Garante was of the opinion that the service providers were in charge of a public service and therefore any event bound by the obligation of secrecy provided by Article 201 of the Code of Criminal Procedure whereby any exemption from obtaining the data subjects’ consent should not be applied.\(^{164}\) In conclusion, the Garante deemed the surveillance activity illegitimate under the Italian Privacy Code, indicating that the processing of personal data must be “lawful[,] and fair[,]”, carried out “for specific, explicit and legitimate purposes”, and “relevant, complete and not excessive in relation to the purposes for which they are collected and subsequently processed.”\(^{165}\)

The opinion of the Garante persuaded the Tribunal of Rome to reject the demands of Peppermint Records.\(^{166}\) On July 14, 2007, the Court of Rome issued a further Court order which rejected the request of Peppermint Records to oblige Wind Telecommunications to disclose users’ data by reiterating the opinion and argument of the Garante.\(^{167}\)

In the aftermath of the judicial proceedings on February 28, 2008, the Garante issued an important decision related to the Peppermint case, which confirmed that it is “illegitimate to ‘spy’

---

162. Id.
163. Id. Contra Sarti, supra note 79, at 441 (arguing that any interpretation giving priority to privacy over intellectual property is inconsistent with community law as set forth in the Peppermint decision).
164. See Trib. di Roma, 14 luglio 2007, n. 1187, AIDA 2007, 1049 (It.).
165. Italian Privacy Code, supra note 158, § 11 (a-b, d).
166. See Trib. di Roma, 14 luglio 2007, n. 1187, AIDA 2007, 1049 (It.).
167. Id.
on the users’ sharing music files and video games” on peer-to-peer systems. The decision is heavily influenced by the Swiss Data Protection Authority opinion in a previous ruling connected to Logistep’s business. Preliminarily, the Garante clarified that the decision only takes into consideration the scanning software activities and not the collateral issues of the disclosure of alleged infringers’ data by the ISPs. Further, the decision is addressed exclusively to Peppermint Records, Techland and Logistep. Despite that, some general principles can be inferred.

The Garante considered the exchange of internet files in light of the notion of communication. The Garante noted that internet file sharing is a private communication falling within the definition of “communication” as per Art. 2, letter (d) of Directive 02/58. This is because, firstly, the number of the recipients is finite. Secondly, file sharing is lacking the simultaneity and uniqueness of transmission that is necessary in public communications. In addition, the Italian Privacy Code supports this conclusion by providing that the exchange of information between a finite number of private subjects through a public communication service shall be considered “electronic communication.”

Therefore, the Garante explained that any processing carried out by internet scanning software technologies should be considered as the monitoring of communications. Such monitoring should be prohibited by Article 5 of Directive 02/58, whereby regular, massive and prolonged monitoring of communications is forbidden to private entities. Further, section 122 of the Italian Privacy Code, supra note 158, § 4(2)(a).
Code provides that the data related to electronic communications can be stored only to help facilitate in supplying the services the user requests and only for the time which is strictly necessary to supply that service. Thus according to the Garante, scanning activity is not required to provide the connectivity service, and therefore, any storage of electronic communication data is unlawful.

The Garante also construed IP addresses to be personal data. Therefore, the processing of the IP addresses shall be governed specifically by sections 11 and 13 of the Italian Privacy Code. Section 11 specifies that personal data undergoing processing shall be "processed lawfully and fairly" and shall be "relevant, complete and not excessive in relation to the purposes for which they are collected or subsequently processed." Therefore according to the Garante, the internet scanning software process is unlawful under Section 11 of the Italian Privacy Code. In fact, the data is communicated by users only for file sharing and is processed only for that specific purpose. On the other hand, the internet scanning software processes the users' data for monitoring objectives aimed at protecting IP rights. This makes any processing excessive in relation to the original collection purposes and is therefore unlawful.

Section 13 of the Italian Privacy Code provides that "[T]he data subject, as well as any other entity from whom or which personal data is collected, shall be preliminarily informed..." as to the data processing if the personal data is collected directly from the data subject. Since internet scanning technologies collect personal

45 (stating that "communication sought by Promusicae of the names and addresses of certain users of KaZaA involves the making available of personal data" and "falls within the scope of Directive 2002/58").
177. Italian Privacy Code, supra note 158, § 122.
178. See GARANTE, supra note 168, § 3 (It.).
179. Id.
181. Id. § 11(1)(a).
182. Id. § 11(1)(d).
183. See GARANTE, supra note 168, § 3 (It.).
184. Italian Privacy Code, supra note 158, § 13(4-5).
data exchanged in peer-to-peer networks, personal data other than the IP codes were collected directly from the users.185 These users did not receive the mandatory preliminary warning as to the data processing.186 Thus, the Garante found the internet scanning software process also unlawful under Section 13 of the Italian Privacy Code.187

5. The Scarlet Case in Belgium

In a landmark case, Société Belge des Auteurs, Compositeurs et Editeurs v. SA Scarlet, the ISP Scarlet was found liable for the unauthorized exchange of music files through its services.188 In June 2007, the Belgian Court of First Instance ordered Scarlet to engage in the blocking and filtering of devices so as to stop the unauthorized exchange of files through peer-to-peer applications.189 Scarlet argued that filtering would infringe upon the privacy rights of its subscribers.190 Rejecting the privacy argument, the Court expressed the opinion that filtering does not handle personal data and is no different from the anti-spam or anti-virus filters that are

---

185. See Garante, supra note 168, at § 3 (IP codes are collected by the "tracker" while all of the other data that is significant in relation to the IP codes -- the file’s information, the date/hour of the download, etc. -- are collected directly by the users).

186. See id.

187. See id.


189. See CARDOZO article, supra note 188, at 1285-89.

190. Id. at 1288.
installed on the ISP’s servers.\textsuperscript{191} In conclusion, the court noted that Scarlet had obtained the permission of all of its subscribers to search their data to prevent illegal activities, rendering the handling of personal data lawful for the purposes of the Belgian authors’ society.\textsuperscript{192} The decision was confirmed in October 2008, awaiting for an appeal hearing.\textsuperscript{193}

However, the case has later escalated to the Court of Justice of the European Union. Reference for a preliminary Judgment from the Court of Appeal of Brussels was lodge with the European Court of Justice on February 5, 2010.\textsuperscript{194} The question referred asked to the European Court of Justice:

Do Directives 2001/29 and 2004/48, in conjunction with Directives 95/46, 2000/31 and 2002/58, construed in particular in the light of Articles 8 and 10 of the European Convention on the Protection of Human Rights and Fundamental Freedoms, permit Member States to authorise a national court, before which substantive proceedings have been brought and on the basis merely of a statutory provision stating that: ‘They [the national courts] may also issue an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right’, to order an Internet Service Provider (ISP) to introduce, for all its customers, in abstract and as a preventive measure, exclusively at the cost of that ISP and for an unlimited period, a system for filtering all electronic communications, both incoming and outgoing, passing via its services, in particular those

\textsuperscript{191} Id. at 1289.

\textsuperscript{192} Id.

\textsuperscript{193} See Press Release, Alex Jacob, Int’l. Fed’n. of the Phonographic Indus., SABAM Case: Court Confirms Scarlet Must Filter or Pay Fines from 1st November (Oct. 31, 2008), available at www.ifpi.org/content/section_news/20081031.html. See also Chris Watson, SABAM v. Tiscali – Questions From Belgian Court to The ECI Published, Cameron McKenna (2010), available at http://www.mondaq.com/article.asp?articleid=94090.

involving the use of peer-to-peer software, in order to identify on its network the sharing of electronic files containing a musical, cinematographic or audio-visual work in respect of which the applicant claims to hold rights, and subsequently to block the transfer of such files, either at the point at which they are requested or at which they are sent?

The decision of the European Court of Justice is awaited. So far, however, an initial stance on the question has been taken by the Advocate General of the European Court of Justice.195 The Advocate General, Mr. Pedro Cruz Villalon found that the order issued by the Belgian Court in the Scarlet case violated several provisions of the Charter of Fundamental Rights,196 including the rights to private communication, protection of personal data, and freedom of information. The Advocate General concluded that for those rights to be abridged the legislature must act first and any Internet restriction must be “adopted on a national legal basis which was accessible, clear and predictable.”197

6. France

The French implementation of the e-commerce directive included specific notice and take down measures requiring ISPs to collect and keep the identification and log data of their subscribers.198 In addition, the 2004 revision of privacy and data


protection legislation granted collecting societies the right to create files with the data of alleged copyright infringers, with the aim of assuring the defense of the authors’ rights. On July 29, 2004, the French Constitutional Court was called to decide on the constitutionality of the new data protection law. By upholding the constitutionality of the law, the Court explicitly rejected the complaint and addressed the issue of rights granted to collection societies. Specifically, the Court pointed out the existence of other safeguards in the law, such as the one-year term of data retention, and declared “the law does not damage in any legal way the constitutional requirement to respect private life.”

The Commission Nationale de l’Informatique et des Libertés (CNIL), the French data protection authority, is working on striking a balance between privacy and copyright. In 2005, CNIL authorized the Syndicat des Editeurs de Logiciels de Loisirs (SELL), a software lobbying organization, to monitor file sharing on peer-to-peer networks, to send instant messages to prevent piracy, and to collect users’ IP addresses in a database. In doing so, CNIL ruled that IP addresses get a “personal character within the framework of a legal procedure.” Shortly after, the Société des Auteurs, Compositeurs et Editeurs de Musique (SACEM), the Société pour l’administration du Droit de Reproduction Mécanique

4&dateTexte=.


201. Id.

202. Id.


204. Id.
(SDRM), the Société Civile des Producteurs Phonographiques (SCPP) and the Société Civile des Producteurs de Phonogrammes en France (SPPF) and other copyright holders' organizations sought the same authorization.205

Unexpectedly, CNIL denied SACEM the requested authorization.206 In doing so, the organization pointed out that ISPs should not collaborate with the copyright owners, and reiterated the Constitutional Court ruling of July 29, 2004, which restricted the use of traffic data to prosecute copyright infringers to the judiciary.207 The CNIL then listed the reasons why the automatic collection of IP addresses was not a proportionate response to copyright infringement, and therefore unlawful.208 First, CNIL stated that allowing organizations to gather IP addresses could lead to the massive collection of personal data. Second, CNIL feared that the proposed data collection could permit extensive and permanent surveillance of peer-to-peer networks. Third, CNIL noted that it was unclear on which basis users should be prosecuted as a result of the collection.209

However, in May of 2007, the Conseil d’Etat (French Supreme Administrative Court) overruled CNIL’s refusal to authorize SACEM’s data collection programs because it did not consider them to be overreaching, especially given the extent of music exchange on the Internet and the limited number of titles under surveillance.210 Still, the Conseil d’Etat did approve the position of

---

207. Id.
208. Id.
209. Id.
CNIL with respect to sending warning messages to persons uploading music. Subsequent to this ruling, CNIL was forced to authorize SACEM and other collection organizations to implement search and detect processes for online copyright infringement.

Slightly before the Conseil d’Etat decision, two decisions by the Paris Court of Appeal took an uncommon stand on the nature of IP codes. In two lawsuits brought against the Société Civile des Producteurs Phonographiques (SCPP) by users allegedly uploading copyrighted music on the Internet, the Court did not deem IP addresses that were collected while searching for infringement activity to be personal data. The CNIL heavily protested against these decisions, and noted that IP addresses are considered personal data by all European data protection authorities. On the urging of CNIL, an appeal against the two decisions is now pending in front of the French Supreme Court. In June 2008, the Court of Appeal of Rennes reaffirmed the nature of personal data of IP addresses by squashing two earlier verdicts, thus convicting two file-sharers because the IP addresses were


211. Id.


215. Id.

216. Id.
illegally obtained. 217 According to this ruling, officers of SACEM and SCPP had collected the IP addresses in an unlawful manner because it was without the prior approval of CNIL. 218 On January 13, 2009, the French Supreme Court squashed the decision of the Rennes’ Court of Appeal. 219 In doing so, the French Court of Cassation did not express a view as to whether an IP address qualifies as personal data. However, it stated that the act of collecting an IP address for the purpose of obtaining the identity of an individual falls within the power of a sworn agent and does not constitute data mining. 220 Thus, the Court of Cassation concluded that it was unnecessary for officers of SCPP and SACEM to seek CNIL approval for collecting IP addresses. 221

Not surprisingly, given the French tradition of protection for authors’ rights since the first CNIL decision, the French government intended to intervene on the implementation of Directive 04/48 to bypass privacy hurdles. 222 The result was the


220. Id.

221. Id.

adoption by the French National Assembly of the so-called “graduated response” or “three strikes” internet policy. The law implements a system of massive tracking and monitoring of internet users and alleged infringers by the creation of an agency, commonly referred to as HADOPI. The aim of the law is to institute a graduated response for alleged copyright infringers on the Internet. As originally drafted, the law empowered the newly created agency to locate infringers, send them warnings of illegal downloading, and apply sanctions including the suspension of internet access after three warnings. However, the original version of the law was struck down by the French Constitutional Court in June 2009. The Constitutional Court found the sanctioning ability of the administrative agency to be unconstitutional because the suspension of internet service can only be decided by a judge. Therefore, the decision of the Constitutional Court left in place the surveillance and warning steps of the graduated response mechanism. Shortly thereafter, the French legislators approved an amended version of the law, known as HADOPI 2. In order to conform to the Constitutional

almost the same content of the ISPs codes of self regulation proposed by the MPA and IFPI. See supra note 46.


224. ld.

225. ld.


227. ld.


Court’s ruling, the amended law restored the penalties subject to a decision by a judge instead of an administrative agency. Nonetheless, the new text was challenged on constitutional grounds by French deputies arguing that the suspension of internet service would jeopardize freedom of speech and communication. The French Constitutional Court gave the green light to HADOPI 2 in October 2009.

7. The BREIN Case in the Netherlands

In 2005, the Netherlands began their first proceeding against individual file sharers. The Bescherming Rechten Entertainment Industrie Nederland (BREIN) foundation, a “joint anti-piracy program of authors, artists and producers of music, film and interactive software,” intended to file lawsuits against the alleged copyright infringers. BREIN sued five Internet Service Providers (“ISPs”) to acquire data for identifying these users. The ISPs decided not to voluntarily provide the requested information due to concerns about liability and claims that any disclosure would

---

230. See Bill 332, supra note 229.
233. See New Wave Of Lawsuits Against European P2P Users, supra note 16.
234. See Wat is BREIN, http://www.anti-piracy.nl/over_brein/wat_is_brein.asp (last visited Sept. 12, 2010).
235. See New Wave Of Lawsuits Against European P2P Users, supra note 16.
236. The five Internet Service Providers referenced are: Planet Internet, Het Net, @Home, Wanadoo and Tiscali.
237. See New Wave Of Lawsuits Against European P2P Users, supra note 16.
violate the Dutch Personal Data Protection Act.\textsuperscript{238} The ISPs argued that the legitimacy of that disclosure should be decided via judicial review.\textsuperscript{239} However the ISPs agreed to forward BREIN’s cease and desist letters to theirs users.\textsuperscript{240} Only a small number of users responded to BREIN’s requests and the case was brought to court.\textsuperscript{241}

On July 12, 2005, the Court of Utrecht, rejected BREIN’s demands\textsuperscript{242} and the Court of Appeal of Amsterdam upheld the lower court’s ruling on July 13, 2006.\textsuperscript{243} However, the decision does not set a clear victory for privacy advocates. After acknowledging IP addresses are personal data under Dutch data protection law,\textsuperscript{244} the court’s rejection of the order of disclosure has been based mainly on the fact that BREIN used an American company, MediaSentry, to collect the data about the infringers.\textsuperscript{245} According to the Court’s ruling, the United States “cannot be regarded as a country with an appropriate level of protection for


\textsuperscript{239} See New Wave of Lawsuits Against European P2P Users, supra note 16.

\textsuperscript{240} See id. Sending fifty letters, BREIN demanded identification of the user, an agreement to pay a fine of 2,100 euros, and an agreement not to be involved in unlawful distribution on the Internet, or else face an additional fine of 5,000 euros per day., See also E-mail from Bescherming Rechten Entertainment Industrie Nederland (BREIN) to ISP, Betreft: Illegale terbeschikkingsstelling muziekbestanden via het Internet vanaf IP-adres (Mar. 31, 2005), available at http://www.bof.nl/docs/breinvordering.pdf.

\textsuperscript{241} See New Wave Of Lawsuits Against European P2P Users, supra note 16.

\textsuperscript{242} See Voorzieningenrechter Rechtbank Amsterdam 12 juli 2005, KGZA 2005, 05-462 m.nt. BL/EV (Foundation/UPC Nederland B.V. et al) (Neth.).

\textsuperscript{243} Hof’s-Amsterdam 13 juli 2005, KG 2005, 1457-1405 m.nt. BL/EV (Foundation/UPC Nederland B.V. et al) (Neth.).


\textsuperscript{245} Foundation/UPC Nederland B.V. et al. [Voorzieningenrechter Rechtbank], supra note 242, at § 2.9.
personal data." 246 Additionally, the court found that, since MediaSentry had not signed a Safe Harbor agreement nor had an authorization under the Dutch Personal Data Protection Act, that it cannot be assumed that MediaSentry took into account the same guarantees as BREIN in its data processing and investigation. 247

Furthermore, by investigating the shared folders, MediaSentry had access to all files containing personal data, including those that were not of the alleged infringers. 248 The Court concluded that BREIN unlawfully collected and processed IP addresses and violated the Personal Data Protection Act. 249 Accordingly, the court ruled that under these circumstances the ISPs must refuse to disclose personal data since they have an obligation to preserve personal data. 250

The privacy protection which was enforced in the BREIN ruling is strongly affected by the peculiarity of the data collector. Under different preconditions, the Court may have reached a different conclusion. In fact, the Dutch Court stated that private parties may demand personal data if they can prove that the IP address is related to the infringers, beyond any reasonable doubt by mentioning date and exact time of the infringing acts. 251 BREIN’s request would have been most likely rejected under this test because BREIN’s cease-and-desist letters had made mistakes concerning the time in which the illegal downloads occurred. 252 Nonetheless, the decision does not ban tout court the disclosure of personal data and the right of disclosure could be granted under the right circumstances.

The Dutch Supreme Court made a further step in easing ISPs’ disclosures when it upheld a decision of the Amsterdam Court of

246. Id. § 4.26.
247. Id.
248. Id.
249. Id. § 4.27.
250. Id. § 4.28.
251. Id. § 4.30.
252. Id. § 4.31 (by making mistakes regarding the time of downloads, innocent users would have been identified; at each session, the ISPs assign a different IP address to the user).
Appeals in the case *Lycos v. Pessers.* In Lycos, the court of Appeals obligated Lycos to provide identifying data of a customer who accused Mr. Pessers of fraud on one of Lycos’ hosted websites. The Supreme Court upheld this decision despite the fact that the accusations on the websites were not “apparently unlawful.” The Courts’ decision if applied liberally, may have simplified the work of the media industry, struggling to obtain personal data of alleged infringers. However, the Supreme Court stressed that this verdict did not constitute a general rule and should be applied only to the specific context of the Lycos litigation.

8. Sweden

Sweden, the country of file shares, the motherland of ThePirateBay, the Pirate Party, and Kazaa, could not be left untouched by the turmoil of the surveillance guerra. In 2005, the Swedish Data Inspection Board ruled that Antipiratbyrån (APB), an anti-piracy group defending the rights of the major content distributors, violated Swedish data protection law. Several

253. See Hoge Raad der Nederlanden [HR] [Supreme Court of the Netherlands], Nov. 25, 2005, AU4019 C04/234HR (Neth.), Lycos Netherlands B.V./Pesser, available at http://zoek.rechtspraak.nl/resultpage.aspx?snelzoek=nl&amp;searchtype =lnl&lt;lnl=AU4019&amp;u_lnl=AU4019; Lycos Netherlands B.V./Pesser, Gerechtshof [Hof] [Court of Appeal] te Amsterdam, 24 juni 2004, KG 1689/03 (Neth.), available at http://www.solv.nl/nieuws_docs/1057Hof%20Adam%2020240604%20%28Lycos-Pessers%29.pdf (in this case, Mr. Pessers offered stamps for sale on eBay; one of Lycos users accused Pessers of fraud and, Mr. Pessers demanded that Lycos divulge the personal data of the offender in order to take legal action against him; Lycos denied the request and was sued by Pessers).

254. Lycos Netherlands B.V./Pesser, Gerechtshof [Hof] [Court of Appeal] te Amsterdam, *supra* note 253.

255. Lycos Netherlands B.V./Pesser, Hoge Raad der Nederlanden [HR] [Supreme Court of the Netherlands], *supra* note 253; see Directive 00/31, *supra* note 42, art. 14(1)(a) (stating that Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that: (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent) (emphasis added).

256. Datainspektionen [Data Inspection Board], *Beslut efter tillsyn enligt*
internet users complained about Antipiratbyråns practice of recording IP addresses, alias, file names, and servers’ locations in order to obtain the disclosure of users’ identities from ISPs.257 Ruling on the complaints, the Data Inspection Board found that an IP address has to be classified as personal data when it can be linked to a person, and the anti-piracy group, as any other private enterprise, did not have any right to collect data, thus infringing upon data protection law.258 The Board pointed out that only government agencies may store that kind of information in criminal cases.259 However, the Board stated also that, under specific circumstances, an organization may apply for an exemption from data protection law.260 At the end of 2005, the Data Inspection Board granted the exception to APB and IFPI.261 The exception expired at the end of 2008.

This initial skirmish was just the prelude to the battle that is being fought today. After the decision of the Data Inspection Board, the Antipiratbyrå lodged an appeal before the County Administrative Court and then again before the Administrative Court of Appeal.262 Both Courts restated that IP addresses are


257. See Lambers, supra note 256.

258. See Data Inspection Board, supra note 256.

259. Id.

260. Id.


262. Länsrättens I Stockholm Län [LR] [County Administrative Court] 2006-12-27, ref.24 (Swed.), available at
personal data and that the activities of Antipiratbyrån were against the Swedish Personal Data Act.\textsuperscript{263} Finally, the Swedish Supreme Administrative Court denied the hearing of the case and therefore upheld the previous decision.\textsuperscript{264}

Meanwhile, on April 1, 2009, the Swedish Parliament passed a law giving copyright holders the right to require ISPs in order to disclose details of file sharers.\textsuperscript{265} The law implements the European Directive 04/48 in Sweden.\textsuperscript{266} Therefore, notwithstanding the ruling of the Supreme Administrative Court, the rightholders do not need to be granted any exception from the Swedish Personal Data Act to collect connection data and retrieve the names of the IP address holders from the ISPs.\textsuperscript{267} As such, the new law enables rightholders


263. Id.


265. Civilrättsliga sanktioner på immaterialrättens område – genomförande av direktiv 2004/48/EG [Civil penalties for intellectual property – The Implementation of Directive 2004/48/EC] Bill 2008/09:67; see also Solna Tingsrätt [TR] [District Court of Solna] 2009-06-25, No. 2707-09 (Swed.), available at http://oppassande.se/bilder/solna_tingsratt/2707-09.pdf (being the first ruling on the new IPRED and deciding that the Swedish ISP ePhone must disclose users’ identities based on the IP addresses given by five audiobook publishers; ePhone was asked by the publishers to reveal the identity of the owner of a server possibly storing hundreds of audiobooks); Svea Hovrätt [HovR] [Court of Appeal of Svea] 2009-10-13, ref OA 6091-09 (Swed.), available at http://www.domstol.se/templates/DV_Press___11317.aspx (court press release) (overruling the Solna District Court decision on the grounds that it was not a matter of copyright infringement since access to the server was password protected, and thus the content was not made publicly available).


267. See David Jonasson, Favorable Court Ruling Do Not Save File-Sharing, STOCKHOLM NEWS, (June 18, 2009), http://www.stockholmnnews.com/more.aspx?NID=3440 (quoting Jonas Agnvall, jurist at the Data Inspection Board, stating “I have not scrutinised the directive in detail, but as I understand they no longer need the legal exception with the implementation of the IPRED-law.”).
to request user information relating to file shares from the ISPs, however the ISPs retain the right to destroy any information about their users, at least until Sweden implements the data retention directive. This leaves two scenarios open. Some ISPs may decide to cooperate with the media industry. Other ISPs may decide not to do so, either because they believe that the privacy of their users must be protected, or because they are afraid of jeopardizing their business. What is certain, so far, is that in Sweden the new law has reduced internet traffic by one-third after going into effect.


In European common law systems, the privacy of file sharers does not enjoy strong protection because of a highly influential precedent decided by the House of Lords in 1973. The Norwich Pharmacal case established the following principle:

if through no fault of his own a person gets mixed up in the tortious acts of others so as to facilitate their wrongdoing, he may incur no personal liability but he comes under a duty to assist the person who has been wronged by giving him full information and disclosing the identity of the wrongdoers.

Under Norwich Pharmacal, the ISPs should come under a duty to assist by providing the means of communication. The Norwich Pharmacal ruling has become a precedent universally followed in law systems that migrated from the UK to Canada, to the U.S. and most recently to Ireland.


272. Id.
In 2004 and 2005, in response to lawsuits filed by the BPI against alleged internet pirates, the English judiciary ordered ISPs to provide the BPI with names and addresses of individuals suspected of uploading large quantities of illegal material to the Internet. Judge Blackburne of the High Court of England and Wales issued an order of disclosure based on the Norwich Pharmacal precedent.

Nonetheless, serious doubts still remain on the standing of the Norwich Pharmacal ruling under the present legislative framework. Article 8 of the European Convention of Human Rights, implemented by the UK Human Rights Act of 1998, states that “everyone has the right to respect for his private and family life, his home and his correspondence.” Following that implementation, Lord Justice Sedley, in Douglas v. Hello! Ltd, commented that “we have reached a point at which it can be said with confidence that the law recognizes and will appropriately protect a right of personal privacy.” It can be argued that the use of the jurisprudence of the European Court of Human Rights coupled with the Human Rights Act of 1998 has created the preconditions for the evolution of an actionable right to privacy in British law. In 1998, the Human Rights Act was enacted in the United Kingdom, in addition to the Data Protection Act, which


276. Id. § 110.

implemented Directive 95/46/EC. However, the data protection law may offer less protection. The 1998 Act states that "personal data may be communicated to third parties for the purpose of, or in connection with, any legal proceedings." The norm leaves open an array of possible interpretations that could lead to the exclusion of protection in the case at issue. Additionally, an application of the Norwich Pharmacal precedent to ISPs seems contrary to the disposition of Directive 00/31/EC on electronic commerce. According to Article 15 of the directive, no obligation to monitor can be imposed on service providers. Under these preconditions, it appears that the Norwich Pharmacal ruling may lose some of its strength.

The debate has been recently fired up by a recent High Court order demanding disclosure of several thousand names and addresses of UK ISP subscribers. The order targeting several ISPs, including British Telecommunications, Orange, and Tiscali was given upon request of the German anti-piracy firm Digiprotect. Digiprotect, together with the law firm Davenport Lyons, acted on behalf of several computer game companies and other content owners. Following this order, Davenport Lyons sent letters to the addresses it obtained demanding a few hundred pounds to avoid legal proceedings. Davenport Lyons' strategy was soon labeled as outrageous, and their campaign was threatened with litigation. It turned out that the data provided to identify the alleged infringers was not accurate and included many innocent bystanders. Soon thereafter, the gaming industry dumped the anti-piracy campaign that was run on its behalf by Davenport Lyons.

279. Digiprotect v. Be Un Limited, [2008 ] EWHC (Ch) 40 (Eng.).
Ireland has also been involved in the debate surrounding privacy and copyright protection. A recent case dealt with the Irish Recorded Music Association’s request for disclosure of the identities of several alleged infringers from their ISPs.  

Unlike the Dutch ISPs sued by BREIN, Eircom and BT decided not to oppose the proceedings. The Irish ISPs only filed for an affidavit to influence the discretion of the court in balancing the rights of consumers against copyright holders. The Irish Court ruled in favor of the music industry and ordered the disclosure of the alleged infringers’ names. Following the Norwich Pharmacal precedent, Justice Kelly of the Court of Dublin ruled that, on the evidence of a prima facie demonstration of copyright infringement, the right of confidentiality “cannot be relied on by a wrongdoer.” The Court explicitly stated that “[t]he right to privacy or confidentiality of identity must give way where there is prima facie evidence of wrongdoing.” However, the Court, quoting the Megaleasing case, pointed out that “[t]he remedy should be confined to cases where every proof of a wrongdoing exists and possibly ... to cases where what is really sought is the names and identity of the wrongdoers rather than the factual information concerning the commission of the wrong.” Finally, the Irish


284. Id.; Mary Carolan, BT, Eircom Will Not Block Firms in File-Sharing Case, THE IRISH TIMES, June 5, 2005, at 17.


286. Norwich Pharmacal, A.C. 133 at 265.


288. Id.

Court cited a recent Canadian case that was also decided on the basis of the Norwich Pharmacal precedent, by specifically agreeing with the Canadian Court when it said:

in cases where plaintiffs show that they have a bona fide claim that unknown persons are infringing their copyright, they have a right to have the identity revealed for the purpose of bringing action. However, caution must be exercised by the courts in ordering such disclosure, to make sure that privacy rights are invaded in the most minimal way.  

This caution may not have been entirely exercised by the Irish Court, though. As in the BREIN case, Irish Recorded Music Association (IRMA) has also employed the American company, MediaSentry, to carry on investigative work. This may entail a breach of the Data Protection Act, as the information concerned was personal data and could be transferred to MediaSentry in the United States only under the Safe Harbor scheme, which was not in place. Under Norwich Pharmacal and Megaleasing, the order of disclosure can be refused if the seeker is guilty of some wrongdoing in connection with the litigation. Because IRMA was in breach of the Data Protection Act, it turns out that it did not come to court with “clean hands” and the order of disclosure should have been refused.

V. CONCLUSIONS

The digital dilemma is still an open question. Privacy and copyright struggle for an answer. Although the entertainment industry claimed to have suspended its litigation campaign, the dead bodies are still on the battlefield. The copyright trolls are raising, both in Europe and the United States, and the future of digital content protection may still lie in mass letter writing and lawsuit campaign. What is of greater concern, however, is that

290. BMG Canada 4 F.C.R. at 105 (Can.).


reconciliation is still a fading mirage. The tension between right of privacy and copyright is substantial and the demand for a solution remains unanswered.

The many parties are relentlessly lobbying for an equilibrium favorable to their own interests. Privacy authorities, quite predictably, and judicial authorities, more surprisingly, show a consistent trend upholding a careful consideration of privacy concerns. Governments, predictably as well, are unresponsive to concerns by strictly abiding to the mantra of the steady enlargement of copyright in the face of any counter-posing interests. The result is a stalemate that makes it difficult to find a fair balance between privacy and copyright. Is the war code to be implemented to face the threat of pirates, their peers and networked vessels? Or should constitutional principles still apply and shield the alleged infringers?

The biggest fear of users lies in the alliance between copyright owners and ISPs to create a parallel justice, which is independent from judicial power. In Europe, that possibility appears unlikely after an agreement was reached on the Telecoms Reform Package, which should now include a provision that guarantees "the principle of presumption of innocence and the right to privacy" and the respect of the European Convention for the Protection of Human Rights and Fundamental Freedoms. 293 This provision

---

293. See Proposal For a Directive Of The European Parliament and of the Council Amending Directives 2002/21/EC on a Common Regulatory Framework for Electronic Communications Networks and Services, 2002/19/EC On Access To, And Interconnection Of, Electronic Communications Networks And Services, And 2002/20/EC on The Authorization Of Electronic Communications Networks and Services, EUR. PARL. DOC. (COM 697 rev1) (2007) [hereinafter Telecoms Reform Package] (proposal from EU Commission to reform the EU’s regulatory framework for electronic communications networks and services with an aim toward completing the internal market for electronic communications); see also Compromise On Amendment 138. Telecom Package Finalized, EDRI-GRAM (Nov. 5, 2009), http://www.edri.org/edrigram/number7.21/amendment138-replaced-consiliation (following hot debate, an agreement on an amendment to the Telecoms Reform Package on measures to be taken by EU Member States regarding end-users’ access to or use of services and applications through electronic communications networks was reached on November 5, 2009).
should explicitly rule out any collection of IP addresses by private entities policing P2P networks for copyright infringement. However, European national courts have already come down to the same conclusion, most recently in the LSG v. Tele2 case decided by the Austrian Supreme Court and the Logistep decision handed over by the Swiss Supreme Court.

Nonetheless, initiatives like the French three strikes policy are becoming much more popular among governments. Though those initiatives must comply in Europe with the right to a “prior fair and impartial procedure” as well as the presumption of innocence, their implementation endangers users’ rights. In particular, it is debatable whether the storage of a massive quantity of users’ data by governmental agencies is necessary and proportionate to the scope of copyright protection. Further, it is doubtful whether there is any proportionality between copyright infringement and the penalty of disconnection inflicted. The doubt is substantiated by the broad recognition of the status of fundamental rights to the right of access to the Internet. Finally, the uncertainty regarding the coincidence between infringer and the account to be blocked makes the three strikes policy a potentially dysfunctional enforcement tool. All in all, three strikes policies make a crucial error in perception. They equate the loss of fundamental civil rights with economically sensible but trivial private interests.

294. Id.; see also Conseil constitutionnel [CC] [Constitutional Court] decision No. 2009-508DC, supra note 226.

295. See Monika Ermert, Council of Europe: Access To Internet Is A Fundamental Right, IPWATCH (June 8, 2009), http://www.ip-watch.org/weblog/2009/06/08/council-of-europe-access-to-internet-is-a-fundamental-right; Marshall Conley & Christina Patterson, Communication, Human Rights and Cyberspace, in HUMAN RIGHTS AND THE INTERNET 211, (Steven Hick, Edward F. Halpin & Eric Hoskins eds., Macmillian Press 2000) (arguing that Internet access is a fundamental value because the Internet, by facilitating the spreading of knowledge, increases freedom of expression and the value of citizenship); Barack Obama, President of the United States, Remarks at Town Hall Meeting With Future Chinese Leaders (Nov. 16, 2009) (stating that “freedom of access to information is a universal right”).