European Commission
DG Internal Market and Services

Study on Online Copyright Enforcement and Data Protection in Selected Member States

November 2009

Prepared by Hunton & Williams, Brussels

Christopher Kuner
Cédric Burton
Dr. Jörg Hladjk
Olivier Proust

For DG Internal Market of the European Commission

With the assistance of
Dr. Andreas Manak, Manak & Partners
Javier Aparicio Salom, Cuatrecasas, Gonçalves Pereira
Ann-Charlotte Högberg, Mannheimer Swartling Advokatbyrå

HUNTON& WILLIAMS

TABLE OF CONTENTS

I. INTRODUCTION AND METHODOLOGY

This study provides an overview of the legal situation regarding the interaction between online copyright enforcement and data protection at the European Union level and in six selected EU Member States, namely Austria, Belgium, France, Germany, Spain and Sweden. It has been prepared on behalf of DG Internal Market and Services of the European Commission by the Brussels office of Hunton & Williams, with the assistance of local counsel, and in the context of the "Stakeholders' Dialogue on Illegal Uploading and Downloading" organized by DG Internal Market and Services. This study was purposely kept brief, and is not intended to provide an exhaustive analysis.

The first section provides a brief overview of the legal instruments relevant to online copyright enforcement and data protection, and of whether the European legal framework for data protection presents a barrier to the fight against online copyright infringement. In particular, this section analyzes the relationship between the various European legal instruments and identifies any legal obstacles to online copyright enforcement. Issues concerning the Data Retention Directive are not analyzed in detail.

The second section analyzes issues regarding the interaction of data protection and online copyright enforcement in six selected EU Member States as of September 1, 2009. The methodology of preparing this section was as follows: a questionnaire was drafted by Hunton & Williams and approved by the European Commission. Hunton & Williams then completed the questionnaire for three countries (Belgium, France, Germany), and instructed local counsel with regard to the others. Hunton & Williams then coordinated and reviewed the work of local counsel, including clarification of important legal points, before finalizing the study.

It is important to realize the limitations of this study. It does not constitute legal advice, and decisions in a particular case should not be based on the study without consulting counsel. While great effort has been put into making the study as accurate as possible, many of the legal concepts and questions examined have not been the subject of authoritative decisions by courts or data protection authorities (DPAs) in some of the countries, so that there is a lack of legal certainty about them. In addition, certain concepts may be understood differently in different countries. Thus, some of the positions and descriptions contained in the study represent our interpretation of the legal situation, rather than a definitive statement of the law. Finally, it was necessary to limit the study to the questions raised in the questionnaire in order to keep the study to a manageable size.

II. AUTHORS OF THE STUDY

Principal Authors:

Hunton & Williams
Park Atrium
Rue des Colonies 11
1000 Brussels
Belgium

Christopher Kuner, Partner (overall responsibility for the study)
E-mail: ckuner@hunton.com

Cédric Burton, LL.M., Avocat au Barreau de Bruxelles (for Belgium, and coordination of the study)
E-mail: cburton@hunton.com

Dr. Jörg Hladjk, LL.M., Rechtsanwalt (for Germany)
E-mail: jhladjk@hunton.com

Olivier Proust, LL.M., Avocat à la Cour (for France)
E-mail: oproust@hunton.com

For Austria:
Dr. Andreas Manak
Manak & Partner, Rechtsanwälte
Stephansplatz 6
1010 Wien
Austria
E-mail: manak@manak.at

For Spain:
Javier Aparicio Salom
Cuatrecasas, Gonçalves Pereira
Velázquez 63
28001 Madrid
Spain
E-mail: javier.aparicio@cuatrecasas.com

For Sweden:
Ann-Charlotte Högberg
Mannheimer Swartling Advokatbyrå AB
Box 1711
111 87 Stockholm
Sweden
E-mail: ach@msa.se

III. EXECUTIVE SUMMARY

As confirmed by the European Court of Justice in the Promusicae and Tele2 judgments, there is no direct legal conflict as such between the European legal framework for data protection and online copyright enforcement. However, the Court's decisions leave open several important questions, such as how to apply the proportionality principle in practice, and how to strike a fair balance between the various rights involved. These issues thus seem to be left to the Member States, and there is little or no harmonization of them at the EU level.

With regard to the legal situation in the six Member States examined, the following general observations can be made:[1]

- IP addresses are generally considered by DPAs and courts to be personal data, although courts in some countries (e.g., France) have taken conflicting positions on this issue.

- IP addresses are generally considered to be traffic data, which means that they may only be processed in a limited number of circumstances and for specific purposes (such as billing, invoicing, etc.), and that consent is generally required to process them for other purposes (such as online copyright enforcement).

- IP addresses processed in the context of online copyright enforcement may be considered to be sensitive data (judicial data), except in Spain.

- ISPs cannot store IP addresses for the specific purpose of online copyright enforcement (except in France, where retention for the purpose of making information available to the judicial authorities or to the Hadopi Commission is allowed).

- The processing of IP addresses by ISPs to pass on infringement warning notices is generally prohibited or subject to strict restrictions (e.g., in France if the Hadopi Act is complied with).

- The general monitoring of P2P networks by right holders resulting in the creation of a database of potential copyright infringers is usually prohibited.

- The disclosure of P2P users' identities by ISPs to judicial authorities in the context of criminal proceedings is generally authorized.

- The disclosure of P2P users' identities by ISPs to right holders for civil enforcement is generally restricted by data protection law. In particular, ISPs may generally not disclose P2P users' identities to right holders outside the context of judicial (administrative) proceedings.

- In most Member States, it seems that little consideration was given to the interaction between data protection rules and implementation of the IP Enforcement Directive.

[1] These represent superficial summaries of complex legal issues that are dealt with in more detail in section V.

IV. OVERVIEW OF THE EUROPEAN LEGAL FRAMEWORK

The European legal framework for online copyright enforcement and data protection is based on the following legal instruments:

- "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data", which sets forth the foundation of data protection law in the European Union (hereinafter referred to as the General Data Protection Directive). The Directive sets forth the general principles applicable to the processing of personal data. Of particular importance for the purpose of this study is Article 13, which specifies the situations where Member States may adopt legislative measures to restrict the scope of the obligations laid down in the Directive. Under this article, restrictions are allowed which constitute necessary measures to safeguard "the protection of the data subject or of the rights and freedoms of others"[2] ("the right and freedoms of others" include the protection of intellectual property rights).

- "Directive 2002/58/EC on the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)", which particularizes and complements Directive 95/46/EC with respect to the processing of personal data in the electronic communications sector (referred to herein as the e-Privacy Directive). The e-Privacy Directive was recently amended in the context of the review of the telecommunications package (the text must still be voted in plenary by the European Parliament probably in mid-December 2009). While one of the amendments deals with the so-called "graduated response mechanism", it does not directly impact the questions discussed in this study.

  Of paramount importance for this study is Article 15 of the e-Privacy Directive, which sets forth the situations in which Members States may adopt legislative measures to restrict the scope of the rights and obligations provided therein. Up to the Promusicae decision of the European Court of Justice, it was unclear whether the exceptions stated in Article 15 of the e-Privacy Directive included those laid down in Article 13 of the General Data Protection Directive. However, "the Promusicae ECJ case clarifies that Article 15 of the e-Privacy Directive must be read in conjunction with Article 13 of the General Data Protection Directive, and must therefore be interpreted as allowing Member States to restrict the scope of obligations provided in certain articles of the E-Privacy Directive, when this is necessary to safeguard the rights and freedoms of others, including the right to intellectual property in civil proceedings. This will allow Member States to adopt legislative measures restricting the scope of certain articles of the e-Privacy Directive in appropriate cases."[3]

[2] Article 13(1) g General Data Protection Directive.

[3] Christopher Kuner, 'Data Protection and Rights Protection on the Internet: The Promusicae Judgment of the European Court of Justice', 2008 European Intellectual Property Review, p. 199.

- "Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market" (referred to herein as the e-Commerce Directive).
    - This Directive does not apply to "questions relating to information society services covered by Directives 95/46/EC and 97/66/EC [2002/58/EC]".[4]
    - Recital (14) of the e-Commerce Directive states that "The protection of individuals with regard to the processing of personal data is solely governed by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector which are fully applicable to information society services; these Directives already establish a Community legal framework in the field of personal data and therefore it is not necessary to cover this issue in this Directive in order to ensure the smooth functioning of the internal market, in particular the free movement of personal data between Member States; the implementation and application of this Directive should be made in full compliance with the principles relating to the protection of personal data, in particular as regards unsolicited commercial communications and the liability of intermediaries."
    - Articles 12-14 of the e-Commerce Directive establish a regime of exemptions from liability (Mere Conduit, Caching and Hosting) which ISPs can benefit from, provided that the conditions specified in these articles are complied with.
    - Article 15 (1) of the e-Commerce Directive prohibits Member States from imposing a general obligation on Mere Conduit, Caching and Hosting providers to "monitor the information which they transmit or store, [or] a general obligation actively to seek facts or circumstances indicating illegal activity." However, Article 15(2) specifies that Member States may "establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements."

- "Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights" (referred to herein as the IP Enforcement Directive), which "shall not affect the Community provisions governing the substantive law on intellectual property, Directive 95/46/EC, Directive 1999/93/EC or Directive 2000/31/EC, in general, and Articles 12 to 15 of Directive 2000/31/EC in particular."[5]
    - Recital (15) of the IP Enforcement Directive states that "This Directive should not affect substantive law on intellectual property, Directive 95/46/EC of 24 October

[4] Article 1(5)(b) e-Commerce Directive.

[5] Article 2(3)(a) IP Enforcement Directive.

1995 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures and Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market."

- Article 8 of the IP Enforcement Directive requires Member States to "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: (a) was found in possession of the infringing goods on a commercial scale; (b) was found to be using the infringing services on a commercial scale; (c) was found to be providing on a commercial scale services used in infringing activities; or (d) was indicated by the person referred to in point (a), (b) or (c) as being involved in the production, manufacture or distribution of the goods or the provision of the services […]" However, this right to information "shall apply without prejudice to other statutory provisions which: […] (e) govern the processing of personal data."

- "Directive 2001/29/EC on the harmonization of certain aspects of copyright and related rights in the information society" (hereinafter referred to as the Copyright in the Information Society Directive), which refers to the General Data Protection Directive only in recital 57 (regarding digital rights management). Article 8.3 of the Directive requires Member States to "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."

There seems to be no direct conflict between the various directives. They generally contain clauses that take their interaction into account ("without prejudice" clauses). However, such clauses are often non-exhaustive, which could lead to uncertainties in their implementation and interpretation.[6] At the same time, while accepting that there is no direct conflict between them, certain issues raised by the directives are not wholly clear, thus leading to questions when the directives are implemented, and when the national legislation implementing them have to be applied in practice. Indeed, these issues have led national courts to refer questions to the European Court of Justice.

The following cases of the Court of Justice are highly relevant to these issues:

[6] For example, the IP Enforcement Directive contains interaction clauses to the General Data Protection Directive, e-Commerce Directive and Copyright in the Information Society Directive, but not to e-Privacy Directive.

– Promusicae[7] case: In this case, the Court of Justice dealt with the question of whether Articles 15(2) and 18 of the e-Commerce Directive, Articles 8(1) and (2) of the Copyright in the Information Society Directive, and Article 8 of the IP Enforcement Directive permit Member States to limit the duty of operators of electronic communications networks and services, of providers of telecommunications network access, and of providers of data storage services to retain and make available connection and traffic information generated during the supply of an information society service where it is required in connection with a criminal investigation or the need to protect public safety and national defense, thus excluding civil proceedings. In other words, the question referred to the Court was whether the Member States are allowed under Community law to exclude the possibility of disclosing traffic data relating to copyright infringers in civil cases, while requiring such disclosure in criminal cases.

  On January 29, 2008, the ECJ held that the e-Commerce Directive, the Copyright in the Information Society Directive, the IP Enforcement Directive, and the e-Privacy Directive do not require the Member States to lay down an obligation to communicate personal data in order to ensure effective protection of copyright in the context of civil proceedings. However, the Court also found that Community law requires that, when implementing such directives, the Member States must strike a fair balance between the various fundamental rights protected by the Community legal order. Further, the Court held, when implementing such directives, the authorities and courts of the Member States must not only interpret their national law in a manner consistent with the directives, but also make sure that they do not rely on an interpretation of them which would be in conflict with such fundamental rights, or with the other general principles of Community law, such as the principle of proportionality.

- Tele2[8] case: In this case, the Court of Justice considered the issue of whether Article 8(3) of the IP Enforcement Directive and Articles 6 and 15 of the e-Privacy Directive should be interpreted as not permitting the disclosure of personal traffic data to private third parties for the purposes of civil proceedings for alleged copyright infringements. The Court held that Community law – in particular, Article 8(3) of the IP Enforcement Directive, read in conjunction with Article 15(1) of the e-Privacy Directive – does not preclude Member States from imposing an obligation to disclose to private third parties personal data relating to Internet traffic in order to enable them to bring civil proceedings for copyright infringements. However, the Court also found that Community law nevertheless requires Member States to ensure that, when transposing into national law the e-Commerce Directive, the Copyright in Information Society Directive, the e-Privacy Directive and the IP Enforcement Directive, they strike a fair balance between the various fundamental rights involved. Moreover, the authorities and courts of Member States must not only interpret their national law in a manner consistent with those directives, but must also make sure that they do not rely on an

[7] Productores de Música de España (Promusicae) v. Telefónica de España SAU (C-275/06) [2008] OJ C64/9.

[8] LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v. Tele2 Telecommunication GmbH (C-557/07) [2009] OJ C113/14.

> interpretation of them which would conflict with those fundamental rights or with the other general principles of Community law, such as the principle of proportionality.

The two decisions of the Court of Justice confirm that there is no direct conflict as such between data protection and online copyright enforcement in the European legal framework. The Court found that the European legal framework does not preclude Member States from imposing an obligation to disclose to private third parties personal data relating to Internet traffic in order to enable them to bring civil proceedings for copyright infringements, but also found that it does not require the Member States to lay down an obligation to communicate personal data in order to ensure effective protection of copyright in the context of civil proceedings. Thus, the Court seems to hold that the European legal framework is neutral in this regard.

The European legal framework and its interpretation by the Court of Justice seem to leave open several important questions, such as:

- How to apply the proportionality principle in practice and strike a fair balance between the various rights involved (such as the right to data protection and the right to property); and
- How to implement and apply the rights specified in Article 8 of the IP Enforcement Directive and the rights specified in Article 8.3 of the Copyright in the Information Society Directive.

At the same time these questions must be balanced with considerations such as the following:

- Upholding the right to data protection of Internet users specified in the General Data Protection and e-Privacy Directives; and
- Maintaining the legal regime applicable to ISPs specified in the e-Commerce Directive.

All these issues remain unclear at the European and national levels. These issues thus seem to be left to Member States, and there is little or no harmonization of them at the EU level.

V. NATIONAL SITUATIONS IN SELECTED COUNTRIES

A. Austria

Prepared by:
Dr. Andreas Manak
Manak & Partners
Vienna, Austria

Table of legislation

Denomination	Reference
DPA	Österreichische Datenschutzkommission
Data Protection Act	Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000)
Telecommunications Act	Telekommunikationsgesetz 2003 (TKG 2003)
Copyright Act	Bundesgesetz über das Urheberrecht an Werken der Literatur und der Kunst und über verwandte Schutzrechte (Urheberrechtsgesetz), BGBl. 111/1936
E-Commerce Act	Bundesgesetz, mit dem bestimmte rechtliche Aspekte des elektronischen Geschäfts- und Rechtsverkehrs geregelt werden (E-Commerce-Gesetz - ECG), BGBl. I Nr. 152/2001
Code of Criminal Procedure	Strafprozessordnung 1975, BGBl. Nr 631/1975

1. Nature of an IP address

1.1 Is an IP address considered to be personal data/traffic data? (Please consider temporary and permanent IP addresses and explain your reasoning.)

An IP address maybe personal data if it may be linked to an identifiable person. In principle, case law and doctrine consider permanent and temporary IP addresses to be personal data. IP addresses are not personal data as such, but they become so when linked to a person's PC although only the hardware is identified, not the particular user. In commercial use, identification could be even more difficult.

Temporary IP addresses, combined with other information like the person's name, user ID or telephone number, may be personal data for the access provider, depending on the relationship with the person. For third parties or other providers, an IP address becomes personal data when information is linked to it. Consequently, an IP address may be personal data for the ISP (§ 4 Z 1 Data Protection Act 2000, DPA recommendation October 11, 2006, K 213.000/0005-DSK/2006).

A permanent IP address is master data but not traffic data. Master data means any personal data required for the establishment, processing, modification or termination of the legal relationships between the user and the provider or for the production and publication of subscriber directories (§ 92 para 3 no 3 Telecommunications Act – TKG 2003).

Regarding temporary IP addresses, the Supreme Court (Decision of July 26, 2005, 11 Os 57/05z, criminal case) did not explicitly classify an IP address as master data, but regarded the name and address of the user linked to the IP address and an information request regarding name and address as concerning master data. This has been supported by some opinions in doctrine *(Schanda,* Auskunftsanspruch gegen Access-Provider über die IP-Adressen von Urheberrechtsverletzern, MR 2005, 18*)*, but there are also strong dissenting opinions *(*also DPA recommendation October 11, 2006, K 213.000/0005-DSK/2006*; Einzinger/Schubert/Schwabl/Wessely/Zykan*, Wer ist 217.204.27.214?, MR 2005, 113*; Wiebe,* Auskunftsverpflichtung der Access Provider, Media und Recht 2005 H 4 Beilage, 1) considering that temporary (dynamic) IP addresses are to be classified as access data and hence as traffic data.

That IP addresses are traffic data has been indirectly acknowledged by the ECJ in the Promusicae case (C-275/06 No. 45). Further, in the case LSG v. Tele2 (ECJ C 557/07 - 19 February 2009) regarding a referral by the Austrian Supreme Court, the Promusicae ruling was confirmed: EC law does not prevent Member States from establishing an obligation to disclose personal traffic data to private third parties for the purpose of civil proceedings for alleged infringements of exclusive rights protected by copyright. The Court reiterated the need to balance fundamental rights and the need for application of the principle of proportionality. This case is also important for confirming that Article 8.3 of Directive 2001/29 (injunctions) applies to Internet access providers.

Based on Decision C 557/07 of the ECJ, the Austrian Supreme Court finally rendered a decision that clarified some of the disputed issues (ruling of 14.7.2009, 4 Ob 41/09x, LSG v. Tele2), and held as follows:

(i) The right holder (RH) (LSG) requested the disclosure of specific data which could only be provided if the ISP (Tele2) processed traffic data. Temporary IP addresses are traffic data. However, traffic data can only be processed for certain purposes on the basis of the e-Privacy Directive and of the Telecommunications Act. Processing for other purposes is not permitted.

(ii) Article 15 of the e-Privacy Directive allows for the protection of right holders (RHs) on the basis of Article 13 (1) of the Framework Data Protection Directive. Member States can permit the storage and processing of traffic data for the provision of information to combat copyright infringements. This is however only possible through legislative measures stating that such traffic data may be stored for a limited period of time. Austrian law does not satisfy these requirements: there is no express provision under which the storage and processing of traffic data is permissible for the purpose of providing information under § 87b para 3 of the Copyright Act.

(iii) Although there is a need for a reasonable balance between the fundamental rights involved, the processing of traffic data by the ISP would be unlawful - and the defendant cannot be placed under an obligation to act in an unlawful manner.

(iv) In conclusion, under the current legal situation, such processing of data and the disclosure of information to the RHs would be unlawful, and the obligation to delete data excludes an obligation to provide the information.

1.2 Is an IP address related to a user committing or facilitating copyright infringement considered to be sensitive data, i.e., judicial data? If so, what is the legal basis for this conclusion and does that regime imply any restrictions, e.g., processing only with consent of the user?

An IP address may be judicial data if it relates to a user's copyright infringement. Judicial data covers not only data about convicted persons, but also about alleged criminals, suspects and defendants. Processing of such data is allowed only if one of the four exceptions contained in the law applies (§ 8 Data Protection Act):

(i) there is an explicit legal obligation or privilege for the processing of the data;

(ii) the person has consented to the processing of the data and has the right to withdraw consent at any time;

(iii) vital interests of the person require the processing; or

(iv) predominant interests of the processor or third parties require the processing.

2. Processing and retention of IP addresses by ISPs

2.1 Can an ISP store IP addresses and subscribers' details when those data are no longer needed for the purposes of the transmission of the communication? If so, can the ISP keep the data for the purpose of fighting online copyright infringement?

Basically, the ISP can store subscribers' details longer than needed for the purpose of the transmission if the details are deemed to be "master data." However, ISPs can store them for limited purposes only. The fight against online copyright infringement is not mentioned explicitly. However, if the data are stored legitimately, pursuant to the recent ruling of the Supreme Court, the legal obligations to disclose (such data as in § 87b Copyright Act and § 18 para 4 e-Commerce Act) would apply (LSG v. Tele2). In any case, the operator has to erase the master data at the latest upon termination of the contractual relationship with the subscriber. Exceptions are permitted only to the extent that these data are still required to settle or collect charges, handle complaints or comply with other legal obligations (§ 97 para 2 TKG 2003).

Regarding IP addresses, it depends on whether they are considered to be master data (i.e., permanent IP addresses) or traffic data (i.e., temporary IP addresses): permanent addresses may be stored, but temporary addresses must be erased or made anonymous after termination of the connection, unless they are needed for billing purposes (§ 99 para 1 TKG 2003).

Secrecy of electronic communications only applies to traffic data, content data, location data, but not to master data. Therefore, the secrecy of electronic communications does not cover subscribers' details and permanent IP addresses. Temporary IP addresses are considered to be traffic data, and the constitutional provisions of secrecy of telecommunications (Art 10a StGG)

and the right to respect for private and family life (Article 8 ECHR) do apply. The provision on secrecy of communications in the Telecommunications Act (§ 93 para 1 TKG 2003) is also applicable, meaning that recording of temporary IP addresses for purposes other than billing is exceptionally allowed with the consent of all users concerned.

In connection with criminal cases, the Austrian Supreme Court, however, considered that only processing with external effects is relevant for communications secrecy, but that internal processing in the course of an information request does not fall under the scope of communications secrecy (Decision of July 26, 2005, 11 Os 57/05z). This decision has been reversed by the most recent decision in the civil case LSG v. Tele2. According to this latest decision, temporary IP addresses must not be stored, hence no disclosure for the purpose of fighting copyright infringements is possible (see section 1.1).

2.2 If applicable, please differentiate between (1) criminal enforcement by judicial authorities and (2) civil enforcement by right holders (RHs)?

(1) Criminal enforcement by judicial authorities

No, there are no specific regulations that oblige or allow ISPs to store and keep IP addresses and subscribers' details for criminal enforcement by judicial authorities. Only the general provisions regarding the storage of master data and traffic data apply. As the Supreme Court pointed out in the ruling LSG v. Tele2, the Austrian legislator has not implemented the exception of Article 15 (1) of the e-Privacy Directive. This provision allows Member States to adopt legislative measures determining the retention of data for a limited period, e.g., for criminal enforcement. Some other provisions establish a right of disclosure to judicial authorities, but no obligation or right to store data (§ 135 para 2 Code of Criminal Procedure). The requested data have to be available already and must have been stored in compliance with the Telecommunications Act. Therefore, ISPs might not be able to disclose the data at the time of the request if they have already deleted the data because of the obligation of erasure (§ 97 TKG, § 99 TKG).

The reform of criminal procedure law implemented on January 1, 2008 removed the possibility to bring a private criminal action ("Privatanklage") without knowing the identity of the infringer (§ 71 Code of Criminal Procedure). A private criminal procedure has to list the name of the infringer (see *Edthaler/Schmid*, Medien und Recht 2008, 220). The right holder is now left with civil information claims under copyright law which are not effective in case of temporary IP addresses. The Ministry of Justice has sent out a draft for an amendment to the Code of Criminal Procedure, which should fill this obvious lack of enforcement rights to some extent. The time limit for official comments to the draft expired on September 25, 2009. Moreover, the question of copyright enforcement has received some attention in connection with the plans of the Ministry of Transport, Innovation and Technology for the implementation of the EU Data Retention Directive. There are strong indications that disclosure of traffic data will be restricted to major criminal offences, which would exclude copyright infringements.

(2) Civil enforcement by RHs

No, there are no specific regulations allowing or requiring ISPs to store or keep IP addresses and

subscribers' details for civil enforcement by RHs. There are regulations regarding the disclosure of such data (§ 87b Copyright Act, § 18 para 4 e-Commerce Act). However, these disclosure obligations are rendered useless in cases where no data can be stored legitimately or if the disclosure is restricted to major offences.

2.3. Can ISPs process IP addresses to pass on infringement warning notices to users? If so, under what conditions (consent, etc.)?

ISPs may not process IP addresses to pass on infringement warning notices to users. Permanent IP addresses are master data and are not covered by the secrecy of electronic communications (§ 93 para 1 Telecommunications Act). Master data may only be collected and processed for the following purposes (§ 97 para 1 Telecommunications Act): (1) conclusion, execution, modification or termination of the contract with the subscriber; (2) subscriber billing; (3) preparation of subscriber directories; and (4) provision of information to emergency services. The sending of notices to users is not a permitted type of processing. Even tighter restrictions apply for temporary IP addresses. None of the exceptions to the purpose limitation of § 97 para 1 Telecommunications Act seems to be wholly applicable.

3. Monitoring of the Internet (in particular of P2P networks)

3.1. Can RHs or their representative(s) monitor/process/filter IP addresses for enforcement purposes? If not, why? If they may, is there any special condition applicable (consent or others)?

Monitoring, investigation, filtering and processing by RHs of temporary IP addresses without additional information are not covered by data protection law since they do not result in the processing of personal data. However, when the RH obtains the user's name and address and links it to a temporary IP address, this IP address is then considered to be personal data, which means it is subject to the same conditions as permanent IP addresses.

Processing of permanent IP addresses is allowed, insofar as it occurs for purposes of prosecution by a public authority and the data are collected legitimately or the data subject has given his consent (§ 4 Z 10 and § 8 para 3 Z 5 Data Protection Act).

Filtering of P2P networks in search of users' IP addresses falls outside the secrecy of electronic communications because the content of such communication is publicly available. However, the collection of temporary IP addresses would be useless, since ISPs are not allowed to store the relevant data to disclose the person to whom this address has been assigned at a certain time.

3.2. If so, can RHs communicate the IP addresses they gathered to the ISPs for the purposes of information requests?

RHs can communicate IP addresses to ISPs for the purpose of identifying the data subject only if three cumulative criteria are satisfied. Data can only be communicated if (1) they originate from data processing in compliance with data protection law, (2) the ISP has satisfactorily demonstrated to the RH his statutory competence or legitimate authority with regard to the purpose of transmission (granted by the right of disclosure under copyright law), and (3) the

interests of the data subject in secrecy are not infringed by the purpose and content of the transmission (fulfilled by the overriding interest of the controller if the use is necessary for prosecution purposes before an authority; for other purposes, the criteria will be whether or not the legitimate interest pursued by the controller or a third party requires the use of the data).

4. Disclosure of the identity of Internet users (in particular of P2P users)

4.1. Can ISPs voluntarily disclose the users' details to RHs in order that they may bring a civil action? If so, under what conditions (consent, etc.)?

Since there are civil claims for disclosure of users' details without the prior decision of a court or other authority, voluntary disclosure is not a relevant issue in Austria (§ 87b Copyright Act, § 18 para 4 e-Commerce Act). For clarification of ISPs' duties under these disclosure claims, special cooperation procedures between ISPs, RHs and the DPA have been established.

The Internet Service Provider Austria (ISPA) Code of Conduct established rules for disclosure and liability of ISPs based on the e-Commerce Act. ISPA also issued a General Code of Conduct covering the regulations of the Telecommunications Act. Moreover, ISPA issued a position paper dealing with disclosure of information whereby a specific IP address was assigned to a person at a certain time.

Under copyright law, ISPs must disclose users' details to RHs in order that they may bring a civil action. For copyright enforcement purposes, the Austrian Copyright Act establishes an obligation of disclosure. The information request must be made in writing, sufficiently substantiated, and state facts that sufficiently warrant the suspicion of infringement by the user (§ 87b para 3 Copyright Act). However, this obligation does not apply to temporary IP addresses (ruling LSG v. Tele2 by the Supreme Court).

Host providers have a duty to disclose the user's identity to third parties (e.g., a collecting society) with an overriding legitimate interest in the determination of the user's identity and concerning a particular illegal issue, and when the knowledge of this information is essential for enforcement (§ 13 and § 18 para 4 e-Commerce Act). § 18 para 4 concerns only host providers. However, the case law of the Supreme Court (4 Ob 7/04i) and the appellate courts (OLG Wien, 5 R 193/06y) suggests differently, and holds that § 18 para 4 is applicable as a basis for information duties of both telecommunications service providers and access providers. In the light of the decision LSG v. Tele2 this extension of the scope of § 18 para 4 is restricted to master data only, and therefore not relevant for temporary IP addresses.

4.2. Is there any procedure in place to compel ISPs to disclose the identity of Internet users suspected of online copyright infringement within the framework of (1) criminal enforcement by judicial authorities or (2) civil enforcement by RHs?

(1) Criminal procedure

The current provisions for the criminal procedure exclude the RHs from any investigation against unknown infringers (§ 71 para 1 Code of Criminal Procedure). An amendment is planned (see section 2.2).

As soon as § 71 Code of Criminal Procedure is amended, § 135 will provide a procedure for the disclosure of the identity of Internet users. However, in case of temporary IP addresses, this procedure will still be ineffective (see LSG v. Tele2 case).

(2) Civil procedure

The obligations of ISPs to disclose user data pursuant to § 18 para 4 e-Commerce Act and § 87b para 3 Copyright Act are enforceable by action in civil courts. This enforcement is not possible if traffic data (temporary IP addresses) are involved (see LSG v. Tele2 case).

B. Belgium

Prepared by:

Cédric Burton, LL.M.
Avocat au Barreau de Bruxelles
Hunton & Williams
Brussels, Belgium

Table of legislation

Denomination	Reference
DPA	Commission de la protection de la vie privée
Data Protection Act	Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993
Electronic Communications Act	Loi du 13 juin 2005 relative aux communications électroniques, *M.B.*, 20 juin 2005
Copyright Act	Loi du 30 juin 1994 relative au droit d'auteur et aux droits voisins, *M.B.*, 27 juillet 1994
IFPI Opinion	Avis d'initiative n° 44/2001 concernant la compatibilité de la recherche d'infractions au droit d'auteur commises sur Internet avec les dispositions juridiques protégeant les données à caractère personnel et les télécommunications, Commission de la protection de la vie privée, 12 novembre 2001

1. Nature of an IP address

1.1. Is an IP address considered to be personal data/traffic data? (Please consider temporary and permanent IP addresses and explain your reasoning.)

An IP address may be personal data. A temporary or permanent IP address may be personal data because it is possible to identify the data subject via the ISP. Identification is necessary to reach RHs' objectives. Therefore, general data protection rules will most likely apply to IP addresses collected for online copyright infringement (Article 1§1 Data Protection Act and IFPI Opinion).

However, on June 29, 2007, the "Tribunal de Première Instance" of Brussels held that the use of filtering and blocking software does not involve the processing of personal data. In particular, the Court considered that filtering and blocking software are technical tools only, comparable to anti-virus and anti-spam software, which as such do not identify Internet users. In addition, even if this would be considered to be processing of personal data, the ISPs would be able to rely on Article 5(b) of the Belgian Data Protection Act (the processing is necessary for the performance of a contract - the contract being the ISPs terms of uses which include the prohibition of using the ISP network for illegal activities, including copyright infringement). This decision is currently under appeal.

An IP address may be traffic data. Article 2 Electronic Communications Act defines traffic data as "any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing of this type of communication." There is no doubt that an IP address is traffic data under Belgian law. Traffic data can only be processed by ISPs for limited purposes listed in Article 122 of the Electronic Communications Act and are covered by the secrecy of electronic communications.

1.2. Is an IP address related to a user committing or facilitating copyright infringement considered to be sensitive data, i.e., judicial data? If so, what is the legal basis for this conclusion and does that regime imply any restrictions, e.g., processing only with consent of the user?

An IP address may be judicial data. Under Belgian law, judicial data is a specific category of sensitive data and is defined as: "personal data relating to litigations that have been submitted to courts as well as to administrative judicial bodies, relating to suspicions, prosecutions or convictions in matters of criminal offences, administrative sanctions or security measures" (Article 8 Belgian Data Protection Act). Therefore, judicial data covers not only data about convicted persons, but also about alleged criminals, suspects and defendants. The DPA considers that "data collected on the Internet [for the fight against online copyright infringement] is data related to suspicions of criminal offences. For this reason, it is judicial data and its processing is prohibited unless strictly regulated exceptions apply" (IFPI Opinion).

The number of situations in which judicial data may be processed is restricted under Belgian law. For example, consent is not a valid legal basis for the processing of judicial data. There are two particular requirements to the processing of judicial data which are relevant for this study. First, the controller must be in a preparatory phase of litigation (no processing of judicial data allowed unless litigation is being prepared). Thus, it is questionable whether the collection of an IP address in order to send a notice to the data subject meets this requirement. Second, the processing may occur only when the litigation of the controller so requires. In principle, the copyright holder is the only person who may conduct this processing. However, a collecting society may process data related to an artist it represents in a judicial action (IFPI Opinion).

In addition, when processing judicial data, the controller must determine the categories of persons who have access to the data and must keep a list of these persons with a precise description of their functions with regard to the data processing; this list must be at the disposal of the DPA. In addition, the persons who have access to the data must be bound by a legal or contractual duty of confidentiality. Finally, at the time of the notification, the legal basis justifying the processing must be indicated (Article 8 Data Protection Act).

However, the Brussels Court held in its decision of June 29, 2007[9], that no personal data were processed when ISPs use filtering and blocking software. In particular, the Court considered that filtering and blocking software are merely technical tools, comparable to anti-virus and anti-spam software, which as such do not identify Internet users. However, the Court did not analyze

[9] Tribunal de première instance de Bruxelles, 29 juin 2007, *A.M.* 2007, liv. 5, 476.

data protection issues in details. Following the Court's reasoning, it may be inferred that there is no processing of sensitive (e.g., judicial) data since there is no processing of personal data at all according to the Court. The decision has been appealed.

2. Processing and retention of IP addresses by ISPs

2.1. Can an ISP store IP addresses and subscribers' details when those data are no longer needed for the purposes of the transmission of the communication?

Since IP addresses are generally considered to be traffic data, ISPs must delete them when they are no longer needed for the purpose of the transmission of the communication (Article 122 §1 Electronic Communications Act). This is also true for subscribers' details when they are considered to be traffic data.

There are a number of exceptions to this general principle, which include billing (Article 122 §2 Electronic Communications Act); marketing of one's own services (Article 122 §3 Electronic Communications Act); fighting fake emergency calls; fraud detection (Article 122 §4 Electronic Communications Act); cooperation with the telecommunications ombudsman in order to identity a person who used maliciously an electronic communications network or service (Article 122 §1, al.2, 1° Electronic Communications Act); and cooperation with competent public authorities for the research or detection of criminal acts (Article 122 §1, al.2, 2° Electronic Communications Act).

As a general rule, the purposes listed above are exceptions to the general principle of deletion and must therefore be interpreted restrictively.

2.2 If so, can the ISP keep those data for the purpose of fighting online copyright infringement?

None of these exceptions explicitly covers online copyright enforcement. Only the following exceptions may seem to be relevant for the purpose of this study and are further analyzed hereunder:

- Detection of fraud (Article 122 §4 Electronic Communications Act). RHs cannot rely on this exception because the data can only be processed and kept for the detection of fraud committed at the expense of an ISP. The preparatory memorandum to the Act mentions the non-payment of the ISP's services as an example.
- Cooperation with competent public authorities for the investigation or detection of criminal offences (Article 122 §1, al.2, 2° Electronic Communications Act). This exception refers to obligations under the Code of Criminal Procedure. In substance, it allows the judicial authorities ("procureur ou juge d'instruction") to order the monitoring, processing and disclosure of traffic data and subscribers' details in case or suspicion of criminal activities (Articles 46bis, §2 and 88bis §2 al. 1 and 3 of the Code of Criminal Procedure). Thus, this exception would apply to judicial criminal enforcement, but could not be relied on for civil enforcement.

The legal framework of these two exceptions is, however, not well defined in Belgian law (Article 126 Electronic Communications Act) since secondary legislation (Royal Decree) was never passed. In particular, no Royal Decree specifies the data retention obligations. In addition, the Ministry of Justice is currently working on a draft bill modifying Article 126 of the Electronic Communication Act and on a draft Royal Decree implementing this article. The Belgian DPA issued a very critical opinion on the initial version of those drafts. However, recently, the Belgian DPA issued a positive opinion on the latest versions.[10] It is not clear whether ISPs will be able to retain the personal data for the purpose of the fight against online copyright infringement.

In any event, under the general data protection legal framework, the data can be used only for the purpose for which they were collected. ISPs may be found in violation of the Belgian Data Protection Act if they use the IP addresses for a purpose other than the ones mentioned above. In addition, the data must be kept in a form which enables identification of data subjects for no longer than what is necessary for the purposes for which the data were collected or for which they are further processed. Therefore, retaining IP addresses and subscribers' details for purposes other than the purposes of the collection will most likely be illegal under Belgian law.

2.3. If applicable, please differentiate between (1) criminal enforcement by judicial authorities and (2) civil enforcement by right holders (RHs)?

(1) Criminal enforcement by judicial authorities

Pursuant to Articles 122 §1, al.2, 2° and 126 of the Electronic Communications Act, ISPs have an obligation to record and store IP addresses and subscribers' details. As mentioned above (see 2.2) the obligation is, however, not well defined under Belgian law.

The disclosure to judicial authorities is regulated by Articles 46bis, §2 and 88bis §2 al. 1 and 3 of the Code of Criminal Procedure. These articles are completed by a Royal Decree specifying the exact modalities of cooperation between ISPs and judicial authorities[11]. This Royal Decree is currently under review and a draft is being prepared by the Ministry of Justice.[12] Recently, the Belgian DPA issued a positive opinion on the latest version.[13] It is however not clear yet what

[10] See for example, Avis n° 20/2009 du 1er juillet 2009 relatif à l'avant-projet de loi et au projet d'arrêté royal en matière de rétention de données et au projet d'arrêté royal relatif à l'obligation de collaboration (A/09/012). http://www.privacycommission.be/fr/docs/Commission/2009/avis_20_2009.pdf.

[11] Arrêté royal portant exécution des Articles 46bis, § 2, alinéa 1er, 88bis, § 2, alinéas 1er et 3, et 90quater, § 2, alinéa 3, du code d'instruction criminelle ainsi que de l'Article 109ter, E, § 2, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques.

[12] Projet d'arrêté royal déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques.

[13] See for example, Avis n° 20/2009 du 1er juillet 2009 relatif à l'avant-projet de loi et au projet d'arrêté royal en matière de rétention de données et au projet d'arrêté royal relatif à l'obligation de collaboration (A/09/012). http://www.privacycommission.be/fr/docs/Commission/2009/avis_20_2009.pdf.

would be the exact process, the guarantee and requirements regarding the disclosure to the judicial authorities.

(2) Civil enforcement by RHs

ISPs can neither store nor keep IP addresses and subscribers' details for civil enforcement by RHs, because those data must be deleted after transmission of the communication (except to satisfy one of the purposes listed as exceptions in Article 122 of the Belgian Electronic Communications Act).

2.4. Can ISPs process IP addresses to pass on infringement warning notices to users? If so, under what conditions (consent, etc.)?

The processing of IP addresses by ISPs to pass on notices to users is subject to several important restrictions. Firstly, restrictions under general data protection law may apply, as do restrictions concerning purpose limitation. ISPs must clearly indicate in their privacy policies and terms and conditions the purpose of the processing (to pass on infringement warning notices to users), and inform data subjects of that purpose. Secondly, IP addresses related to copyright infringement are considered to be judicial data and the DPA has stated that their "collection is not allowed when RHs are searching on the Internet in order to identify Internet users with the objective of contacting them and sending them a notice" (IFPI Opinion). Thirdly, IP addresses are considered to be traffic data and may only be processed by ISPs for specific purposes, which do not include passing on infringement warning notices (Articles 122 to 124 l Electronic Communications Act).

3. Monitoring of the Internet (in particular of P2P networks)

3.1. Can RHs or their representative(s) monitor/process/filter IP addresses for enforcement purposes? If not, why? If they may, is there any special condition applicable (consent or others)?

RHs or their representative(s) may not automatically monitor IP addresses for enforcement purposes (automatic monitoring). Automatic monitoring and investigations which potentially result in creating a list of copyright infringers is exclusively reserved to judicial authorities. RHs are prohibited from systematically and proactively researching personal data on the Internet in order to track down copyright infringement. However, RHs can process data related to a specific copyright violation which they have detected (specific monitoring), but only if the requirements regarding judicial data processing are met (IFPI Opinion).

Filtering by ISPs has been authorized in Belgium since the SABAM v. SCARLET judgment. In that particular case, the judge ordered an injunction against SCARLET to stop copyright infringement on its network by technically prohibiting its client to upload or download any of SABAM's musical works. The order was based on Article 87 §1 of the Belgian Copyright Act as interpreted in light of Article 8.3 of European Copyright Directive 2001/29/EC. The court stated that filtering does not constitute personal data processing as such, and that even if it were considered to be, ISPs would be able to rely on Article 5(b) of the Belgian Data Protection Act (the processing is necessary for the performance of a contract - the contract being the ISP's terms

of uses, which include the prohibition of using the ISP network for illegal activities, including copyright infringement). The case is under appeal.

3.2. If so, can RHs communicate the IP addresses they gathered to the ISPs for the purposes of information requests?

This is not relevant in practice because RHs are not generally allowed to collect and retain IP addresses on a large scale, except in certain limited situations discussed above under 3.1.

4. Disclosure of the identity of Internet users (in particular of P2P users)

4.1. Can ISPs voluntarily disclose the users' details to RHs in order that they may bring a civil action? If so, under what conditions (consent, etc.)?

ISPs may not voluntarily disclose a user's identify to RHs in order that they may bring a civil action. Firstly, restrictions under general data protection law may apply, as do restrictions concerning purpose limitation. ISPs must clearly indicate in their privacy policies and terms and conditions the purpose of the processing (to disclose users' details to RHs in order that they may bring a civil action), and inform data subjects of that purpose. Secondly, IP addresses related to copyright infringement are considered to be judicial data and the DPA has stated that "ISPs may not disclose judicial personal data to a third party except within the framework of a criminal proceeding" (see IFPI Opinion). Thirdly, IP addresses are considered to be traffic data and therefore may only be processed for certain purposes (Articles 122 to 124 l Electronic Communications Act). In summary, ISPs may not disclose judicial personal data to a third party except within the framework of criminal proceedings (see IFPI Opinion).

4.2. Is there any procedure in place to compel ISPs to disclose the identity of Internet users suspected of online copyright infringement within the framework of (1) criminal enforcement by judicial authorities or (2) civil enforcement by RHs?

There is no procedure in place that compels ISPs to disclose the identity of P2P users outside the framework of judicial proceedings. Disclosure to judicial authorities is regulated by Articles 46bis, §2 and 88bis §2 al. 1 and 3 of the Code of Criminal Procedure.

In the context of judicial proceedings for copyright infringement, Article 86ter §3 of the Copyright Act allows the judge to order the defendant to disclose all information in his possession, including the identification of the infringer.

C. France

Prepared by:
Olivier Proust, LL.M.
Avocat à la Cour
Hunton & Williams
Brussels, Belgium

Table of legislation

Denomination	Reference
CNIL	French Data Protection Authority (Commission Nationale de l'Informatique et des Libertés)
Data Protection Act	Loi N°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, telle que modifiée par la Loi n°2004-801 du 6 août 2004
Confidence in the Digital Economy Act	Loi N°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique
Posts and Electronic Communications Code	Code des Postes et des Communications Electroniques
Intellectual Property Code	Code de la propriété intellectuelle
Criminal Code	Code pénal

1. Nature of an IP address

1.1. Is an IP address considered to be personal data/traffic data? (Please consider temporary and permanent IP addresses and explain your reasoning.)

An IP address is traditionally considered to be personal data by the French Data Protection Authority (CNIL). In the context of collecting IP addresses on the Internet to fight copyright infringement, the CNIL has clearly stated on several occasions that an IP address is personal data since it allows indirectly for the identification of a natural person with an Internet subscription. Several French courts of first instance have taken the same position (see, for example, a recent decision of the court of first instance of Paris[14]). If an IP address is personal data, then its collection and processing falls under the scope of the Data Protection Act.[15]

[14] TGI Paris, 3ème chambre, 3ème section, 24 juin 2009. The Court clearly stated that "an IP address is personal data since it corresponds to a number provided by an Internet service provider which identifies a computer connected to the network (…). With regard to the existing technology, this address appears to be the only means enabling to track a natural person who has posted content online".

[15] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

The qualification of IP addresses as personal data is, however, controversial. In two decisions relating to counterfeiting on the Internet, the Paris Court of Appeal took the view that IP addresses collected while researching and evidencing counterfeiting acts on the Internet do not, even indirectly, allow for the identification of the natural persons behind the addresses and therefore do not constitute personal data.[16] Without expressing a clear view as to whether an IP address constitutes personal data, the French Court of Cassation ruled on 13 January 2009 that the act of collecting an IP address manually without using an automatic monitoring device for the purpose of obtaining an individual's identity via his Internet service provider falls within the powers of a sworn agent and does not constitute a data processing activity.

Recent developments in France indicate that an IP address is considered to be personal data. In relation with the adoption of the Hadopi Act, the French Constitutional Council ruled on 10 June 2009 that "the authorization granted to private individuals to collect data enabling to identify indirectly the owners of an access to online communications services to the public leads these private individuals to carry out a data processing activity relating to felonies".[17] According to legal commentators, the Council unofficially admitted that an IP address is personal data.

Furthermore, on 27 May 2009, the French Senate issued a report on "the protection of privacy in the age of digital memories"[18] in which it states that, although the status of an IP address is unclear in France, an IP address is a means to identify Internet users and thus should be considered as personal data. In this report, the Senate calls for a legislative amendment which would unambiguously state that an IP address is personal data.

An IP address is traffic data. Traffic data is defined as "any information made available by electronic communication means that may be recorded by the operator in the course of conveying electronic communications and that is relevant for the purposes provided under the law" (Article R.10-12 of the Postal and Electronic Communications Code, "CPCE"), including:

- "any information allowing for the identification of the user" in the case of criminal offences (Article R.10-13 of the CPCE);
- "technical data that allow for the identification of the user" in the case of invoicing (Article R.10-14 of the CPCE).

1.2. Is an IP address related to a user committing or facilitating copyright infringement considered to be sensitive data, i.e., judicial data? If so, what is the legal basis for this conclusion and does that regime imply any restrictions, e.g., processing only with consent of the users?

---

[16] Cour d'appel de Paris, 27 avril 2007, Anthony G. / SCPP; Cour d'appel de Paris, 15 mai 2007, Henri S. / SCPP.

[17] Décision n°2009-580 DC du 10 juin 2009, JORF n°0135 du 13 juin 2009.

[18] "Rapport d'information fait au nom de la Commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale, par le groupe de travail relatif au respect de la vie privée à l'heure des mémoires numériques", by M. Yves Détraigne et Mme Anne-Marie Escoffier, 27 May 2009, available at : http://www.senat.fr/rap/r08-441/r08-441.html.

Under the provisions of the Data Protection Act, an IP address may be considered to constitute judicial data when processed in connection with copyright infringement.19 Pursuant to Article 9 Data Protection Act, judicial data may only be processed by specific categories of persons authorized by law to process personal data relating to offences, convictions and security measures, including:

(a) the courts, public authorities and legal entities that manage public services, within the framework of their legal remit; or
(b) the representatives of the law for the strict need of the exercise of the functions granted to them by the law; or
(c) the collecting societies or professional associations representing RHs acting by virtue of the rights that they administer or on behalf of victims of infringements of the rights for the purposes of ensuring the defense of these rights, and further to an authorization issued by the CNIL pursuant to Article 25-I-3° of the Data Protection Act.

2. Processing and retention of IP addresses by ISPs

2.1. Can an ISP store IP addresses and subscribers' details when those data are no longer needed for the purposes of the transmission of the communication?

The rules that apply to data retention depend on the nature of the data and the applicable legal text under French law.

(1) Personal data: Pursuant to Article 6(5) of the French Data Protection Act, a data controller may only collect and store personal data "in a form that allows the identification of the data subjects for a period no longer than is necessary for the purposes for which they are obtained and processed."

(2) Traffic data: Pursuant to Article L.34-1 of the CPCE, traffic data must be deleted or anonymized by operators of electronic communications and may only be stored exceptionally for a period of up to one year for the purpose of:
- investigating, detecting and prosecuting criminal offences or copyright infringements, and with the sole purpose of making information available, as appropriate, to the judicial authorities and to the Hadopi[20] (in compliance with Article L.331-12 Intellectual Property Code); or
- invoicing and payment of electronic communications services.

[19] In its Decision n°2004-499, July 29, 2004, the French Constitutional Council ("Conseil Constitutionnel") ruled that, under Article 34-1 of the Posts and Electronic Communications Code ("CPCE"), IP addresses can only be considered to be "personal data" when they are used by judicial authorities in the course of prosecuting criminal offences.

[20] Hadopi is the High Authority for the Circulation of Works and the Protection of Creation on the Internet, which is an independent, administrative authority, founded by the Hadopi Act of 12 June 2009, whose purpose is to protect works against violations of copyright committed on electronic communication networks used to provide online services to subscribers.

(3) Data which enable the identification of any person who has contributed to the creation of a content: Article 6-II of the Confidence in the Digital Economy Act of June 21, 2004 states that the persons whose activity it is to provide access to online communications services to the public must withhold and retain data of the nature that enables the identification of any person who has contributed to the creation of a content or of one of the contents of the services which it provides.[21]

2.2. If so, can the ISP keep those data for the purpose of fighting online copyright infringement?

Under the current legal framework, ISPs do not have a legal duty to fight copyright infringement on the Internet. Under the new provisions of the Hadopi Act of 12 June 2009[22], any individual who is a subscriber to Internet access must verify that this access does not infringe copyright law (Article L.336-3 of the Intellectual Property Code). Any violation of this obligation, however, does not render the subscriber criminally liable.

As mentioned above in section 2.1, ISPs may only retain traffic data exceptionally for a period of one year for the sole purpose of disclosing this information to a judicial authority or to the Hadopi authority investigating a copyright infringement. A sworn agent investigating copyright infringement on behalf of the Hadopi's Commission for the Protection of Rights[23] may request that ISPs disclose data revealing the identity of a web user. For more information on what information the Hadopi can request an ISP to disclose, please see section 3.2 below.

2.3. If applicable, please differentiate between (1) criminal enforcement by judicial authorities and (2) civil enforcement by right holders (RHs)?

(1) Criminal enforcement by judicial authorities

As mentioned in section 1.2 above, IP addresses may be considered under data protection law to be judicial data and may only be collected and processed by authorized persons under Article 9 of the Data Protection Act.

See section 2.1 above relating to traffic data.

(2) Civil enforcement by RHs

[21] The definition of such data as well as the period and conditions of their retention will be set out in a Decree for the application of Article 6 of the Confidence in the Digital Economy Act of June 21, 2004, which is currently being discussed by the French Administrative Supreme Court ("Conseil d'Etat") and has not yet been published. According to a draft of this decree, ISPs would have to retain identification data, including IP addresses, for a period of one year.

[22] Law n°2009-669 of 12 June 2009 in Favor of the Circulation and Protection of Creation on the Internet.

[23] The Commission for the Protection of Rights is a sub-body of Hadopi, which acts upon request of a sworn and certified agent, or a public prosecutor, to investigate facts relating to copyright infringement committed on the Internet.

In France, there is no obligation for ISPs to store IP addresses for civil enforcement by RHs. Under the current legal framework, ISPs may disclose data revealing the identity of a web user either to a judicial authority in the course of legal proceedings or to a sworn agent investigating a copyright infringement on behalf of the Hadopi's Commission for the Protection of Rights. RHs and their representatives cannot cooperate directly with ISPs to obtain from them data identifying the web user for the purpose of copyright enforcement.

2.4. Can ISPs process IP addresses to pass on infringement warning notices to users? If so, under what conditions (consent, etc.)?

No, because of strict restrictions on the processing of judicial data and traffic data (see sections 1.2 and 2.1 above).

Under the current legal framework, the Hadopi's Commission for the Protection of Rights may in the course of an investigation send a letter of recommendation to the owner of a subscription, electronically or via his ISP, reminding him of his legal obligation not to breach any copyright law and requesting that he cease any copyright infringing activity. This letter provides the date and time of the copyright infringement, but does not reveal the content of the protected work. The letter must also indicate the contact details of the Commission enabling the subscriber to provide comments and, if requested, to obtain clarification of the copyright violation.

3. Monitoring of the Internet (in particular of P2P networks)

3.1. Can RHs or their representative(s) monitor/process/filter IP addresses for enforcement purposes? If not, why? If they may, is there any special condition applicable (consent or others)?

Automatic monitoring: Automatic monitoring and investigations which result in a list of copyright infringers is exclusively reserved to judicial authorities and to the Hadopi Commission for the Protection of Rights.[24]

Specific monitoring: RHs representatives (mentioned in Articles L321-1 to L321-13 Intellectual Property Code) can process data related to a specific copyright violation which they may have noticed, but only if the requirements regarding judicial data processing are met. RHs' representatives have a specific status under French law authorizing them to process judicial data. Pursuant to Article 9(4°) of the Data Protection Act, RHs' representatives acting by virtue of the rights they administer or on behalf of victims of copyright infringements, and for the purposes of ensuring the defense of these rights, may process personal data relating to offences, convictions an security measures (i.e., judicial data). This data processing activity must be authorized by the CNIL, as required by Article 25 of the Data Protection Act.

[24] The Hapodi Act of 12 June 2009 authorizes the Commission for the Protection of Rights to process personal data on individuals that are subject to an investigation for infringement of copyright law.

Thus, monitoring is statutorily permitted when done on a selected number of P2P protocols and where proportionate to the scale of copyright infringement activities (French Supreme Administrative Court, judgment of May 23, 2007).

Filtering does not constitute monitoring of networks according to the Olivennes Report, as it is merely a technical act requiring no intervention by the ISPs.

3.2. If so, can RHs communicate the IP addresses they gathered to the ISPs for the purposes of information requests?

RHs' representatives may not communicate IP addresses they collected to ISPs for the purpose of discovering the identity of the user, as ISPs may only respond to information requests issued by a judicial or administrative authority (Hadopi).

Pursuant to Article L.336-2 of the Intellectual Property Code, a first instance court can order, upon request of a right holder (RH) or his representative, any measures necessary to prevent or cease copyright infringement, against any person contributing to such violation, by way of a summary court order ("*référé*").

Upon request of a sworn and certified agent or of a public prosecutor, the members of the Hadopi's Commission on the Protection of Rights must investigate the facts relating to copyright infringement. Pursuant to Article L.331-21 of the Intellectual Property Code, the Commission may obtain, for the purpose of its investigation, any documents, regardless of the support used, including data stored and processed by electronic communications operators, ISPs and hosting service providers. In particular, the Commission can request information from electronic communications operators, including but not limited to the identity, postal address, electronic address and telephone number of the subscriber, that are necessary to establish evidence of a copyright infringement.

4. Disclosure of the identity of Internet users (in particular of P2P users)

4.1. Can ISPs voluntarily disclose the users' details to RHs in order that they may bring a civil action? If so, under what conditions (consent, etc.)?

ISPs may not disclose judicial personal data to a third party except within the framework of judicial or administrative proceedings.

4.2. Is there any procedure in place to compel ISPs to disclose the identity of Internet users suspected of online copyright infringement within the framework of (1) criminal enforcement by judicial authorities or (2) civil enforcement by RHs?

There is both an administrative and a judicial (civil and criminal) procedure in place to compel ISPs to disclose the identity of P2P users.

(1) Administrative proceedings

The administrative proceedings created by the Hadopi Act does not authorize ISPs to voluntarily disclose users' details to the RHs. ISPs may only disclose the user's details upon request and following the requirements set up by the Hadopi Act. See section 3.2. above for more information on mandatory disclosure of user's details to the Hadopi Commission for the Protection of Rights.

(2) Judicial proceedings

Under the current legal framework, ISPs may disclose data revealing the identity of the web user to a judicial authority in the course of legal proceedings. Only that judicial authority is authorized to match the IP address with other data to identify the user. RHs and their representatives cannot currently cooperate with ISPs to obtain from them data identifying the web user for the purpose of copyright enforcement.

RHs may get a summary order issued by a court ("*en référé*" or "*sur requête*") requiring a technical provider to take all appropriate measures necessary to prevent or terminate harm caused by the content of a publicly available online communications service (Article 6-I-8 Confidence in the Digital Economy Act). Pursuant to Article L.336-2 of the Intellectual Property Code, a court of first instance may also order, upon request of a right holder or his representative, any measures necessary to prevent or cease copyright infringement, against any person contributing to such violation, by way of a summary court order ("*référé*"). After a claim has been submitted to the judge, ISPs can only be compelled to disclose the IP addresses of P2P users by a court. The court may authorize the use of IP addresses for the purposes it defines in favor of a right holder. The court may further allow the right holder to access personal data through an ISP. A court may also use the summary procedure ("*référé*") of Article 145 of the Code of Civil Procedure in order to preserve evidence.

D. Germany

Prepared by:
Dr. Jörg Hladjk, LL.M.
Rechtsanwalt
Hunton & Williams
Brussels, Belgium

Table of legislation

Denomination	Reference
DPA	Data Protection Authority
Federal Data Protection Act	Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), das zuletzt durch Artikel 1 des Gesetzes vom 14. August 2009 (BGBl. I S. 2814) geändert worden ist
Telemedia Act	Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179), das zuletzt durch Artikel 2 des Gesetzes vom 14. August 2009 (BGBl. I S. 2814) geändert worden ist
Telecommunications Act	Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch Artikel 2 des Gesetzes vom 14. August 2009 (BGBl. I S. 2821) geändert worden ist
Copyright Act	Urheberrechtsgesetz vom 9. September 1965 (BGBl. I S. 1273), das zuletzt durch Artikel 83 des Gesetzes vom 17. Dezember 2008 (BGBl. I S. 2586) geändert worden ist
Criminal Procedure Code	Strafprozeßordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die durch Artikel 3 des Gesetzes vom 30. Juli 2009 (BGBl. I S. 2437) geändert worden ist

1. Nature of an IP address

1.1. Is an IP address considered to be personal data/traffic data? (Please consider temporary and permanent IP addresses and explain your reasoning.)

An IP address (both dynamic and static) is personal data (from an ISP's perspective) because an ISP can associate the IP address with a specific user. It may be questionable whether right holders (RHs) are able to associate an IP address with a specific user. Leading representatives of DPAs, however, take the view that, regardless of the type of data controller, IP addresses always constitute personal data (Schaar, Datenschutz im Internet, 2002, Rn. 174; Dix, DuD 2003, p. 234-235).

A dynamic IP address is "traffic data" as defined by Section 3 (30) Telecommunications Act ("data collected, processed or used in the provision of a telecommunications service").

A static IP address is not only traffic data, but also customer data, as defined by Section 3 (3) Telecommunications Act ("the data of a subscriber collected for the purpose of establishing, framing the contents of, modifying or terminating a contract for telecommunications services").

Some authorities argue that addresses are given as part of the performance of a contract because ISPs have an obligation to the users to provide the same IP address for every access.

1.2. Is an IP address related to a user committing or facilitating copyright infringement considered to be sensitive data, i.e., judicial data? If so, what is the legal basis for this conclusion and does that regime imply any restrictions, e.g., processing only with consent of the user?

IP addresses may be sensitive data. They are not considered *per se* to be sensitive data, but could become so by a contextual assessment if processed in connection with a user committing criminal offences such as copyright infringement. In such cases, special restrictions apply to the processing. For example, any consent must refer expressly to such data in addition to the usual requirements for consent (i.e., consent must be specific, informed, freely given, explicit, and revocable). The processing of sensitive data for one's own business purposes is admissible when the data subject has not consented if this is "necessary in order to assert, exercise or defend legal claims and there is no reason to assume that the data subject has an overriding legitimate interest in excluding such collection, processing or use." This exception, however, does not apply in cases of enforcement of legal claims of a third party which has no relationship to the data controller (see DPA of Berlin, Annual Report 2002, p. 29).

2. Processing and retention of IP addresses by ISPs

2.1. Can an ISP store IP addresses and subscribers' details when those data are no longer needed for the purposes of the transmission of the communication?

(1) IP addresses

According to Section 96 (2) Telecommunications Act, stored traffic data, such as IP addresses, may be used after the termination of a connection only where required to set up a further connection or for the purposes referred to in Sections 97 (charging and billing), 99 (itemized billing), 100 (Faults in Telecommunications Systems and Telecommunications Service Fraud) and 101 (Information on Incoming Calls), or if necessary for the purposes legitimized by other statutory provisions. Otherwise, traffic data are to be erased by the service provider without undue delay following termination of the connection (Section 96 (1) No. 2 Telecommunications Act).

(2) Subscribers' details

Yes, because "subscribers' details" can be classified as "customer data" as defined in Section 3 (3) Telecommunications Act. Customer data are data of a subscriber collected for the purpose of establishing, framing the contents of, modifying or terminating a contract for telecommunications services. Therefore, they can be stored for those purposes.

2.2. If so, can the ISP keep those data for the purpose of fighting online copyright infringement?

(1) IP addresses

According to Section 96 (2), IP addresses may be used after the termination of a connection only where required to set up a further connection or for the purposes referred to in Sections 97-101 (see 2.1 (1) above) or if necessary for other purposes legitimized by other statutory provisions. Otherwise, traffic data, such as IP addresses, are to be erased by the service provider without undue delay following termination of the connection.

(2) Subscribers' details

According to Section 95 (1) Telecommunications Act, the ISP may collect and use customer data only to the extent required to achieve the purposes of establishing, modifying or terminating a contract for telecommunications services. Transmission of the customer data to third parties, unless permitted by the Telecommunications Act or by another law, can only be carried out with the subscriber's consent.

When the contractual relationship ends, the customer data must be erased by the ISP upon expiry of the calendar year following the year of the contract termination (Section 95 (3) Telecommunications Act). Section 35 (3) of the Federal Data Protection Act applies accordingly with regard to deletion. Therefore, rather than being erased, customer data have to be blocked ("blocking" means labeling stored personal data so as to restrict their further processing or use), in so far as (1) retention periods prescribed by law, statutes or contracts preclude erasure, (2) there is no reason to assume that erasure would impair the legitimate interests of the customer, or (3) erasure is not possible or is only possible with a disproportionately high effort due to the specific method of storage.

2.3. If applicable, please differentiate between (1) criminal enforcement by judicial authorities and (2) civil enforcement by right holders (RHs)?

(1) Criminal enforcement by judicial authorities

Although the criminal enforcement authorities have the possibility to collect traffic data in real time, ISPs also have an obligation to disclose traffic data to these authorities under certain circumstances. This obligation is governed by Sections 100g (2) and 100b (3) of the Code of Criminal Procedure (StPO).

In cases where certain facts give rise to the suspicion that a person, either as perpetrator, or as inciter or accessory, either (i) has committed a criminal offence of substantial significance in the individual case as well, particularly one of the offences referred to in Section 100a (2) StPO ("serious criminal offences"), or, in cases where there is criminal liability for attempt, has attempted to commit such an offence or has prepared such an offence by committing a criminal offence, or (ii) has committed a criminal offence by means of telecommunications, then, to the

extent that this is necessary to establish the facts or determine the suspect's whereabouts, traffic data may be obtained also without the data subject's knowledge (Section 100g (1) StPO).

In the case of committing offences through telecommunications means, the measure is only admissible where other means of establishing the facts or determining the suspect's whereabouts would offer no prospect of success and if the acquisition of the data is proportionate to the seriousness of the case (Section 100g (1) sentence 2 StPO).

The disclosure order must contain the following: (i) to the extent possible, the name and address of the targeted individual, (ii) the phone number or another identifier of the individual's telecommunications connection or device, and (iii) the type, scope and duration of the measure, including its end (Section 100b (2), No. 1-3 StPO). With regard to (ii), in the case of a criminal offence of substantial significance, a sufficiently precise spatial and temporal description of the telecommunication is sufficient where other means of establishing the facts or determining the suspect's whereabouts would offer no prospect of success or would prove much more difficult (Section 100g (2) StPO).

Disclosure of traffic data has to be ordered by a judge. When delay would be prejudicial, the Public Prosecutor's Office may issue the order (Section 100b (1) second sentence). The order issued by the Public Prosecutor's Office expires unless it is confirmed within three days by a judge (Section 100b (1) third sentence, StPO). The order has to be issued in writing. Its validity has to be limited to a maximum of three months, with the possibility of extension for additional maximum periods of three months at a time if the conditions which led to its issuance remain unchanged (Section 100b (1) third sentence, StPO). The persons concerned, i.e., in particular those who are the subject of the order, are to be notified that information is being disclosed as soon as this can be done without endangering the purpose of the investigation, the life, physical integrity and personal liberty of another person, or significant assets (Section 101 (5) first sentence, StPO). Several state public prosecutors have published guidelines for investigating file sharing that include differences regarding the threshold for the initiation of copyright infringement prosecutions.

(2) Civil enforcement by RHs

On September 1, 2008, the law implementing the IP Enforcement Directive (2004/48/EC) came into force. According to Section 101 (1) of the Copyright Act, right holders may now bring a claim to request disclosure of the identity of users. The condition for bringing such a claim is that there has been a breach of copyright on a "commercial scale". The commercial scale may be determined by the number of violations as well as their gravity. In addition, the breach is limited to "obvious" cases and requires that a claim has been brought by the RH against the infringer. So far, courts have interpreted what constitutes a breach "on a commercial scale" in various ways. The annex to this section summarizes some cases by regional courts, which demonstrate the varying approaches to the definition of "commercial scale".

Section 113b Telecommunications Act contains restrictions that make it practically impossible to bring claims under civil law. The only data that could be disclosed under Section 101 Copyright Act are the data that the provider stores for billing purposes. Such data, however, must be deleted

in accordance with Sections 96 (2) and 97 (3) sentence 3 Telecommunications Act as soon as they are no longer necessary for these purposes. The restrictions of Sections 113b Telecommunications Act also apply to dynamic IP addresses necessary to prove participation in P2P networks. In summary, Section 101 Copyright Act therefore was intended to strengthen RH rights, but the enforcement of such claims is extremely limited in most cases.

2.4. Can ISPs process IP addresses to pass on infringement warning notices to users? If so, under what conditions (consent, etc.)?

No, a legal basis or consent is necessary. Consent may not be obtained via an ISP's terms and conditions and implied consent is not valid. In addition, ISPs face restrictions due to telecommunications secrecy.

3. Monitoring of the Internet (in particular of P2P networks)

3.1. Can RHs or their representative(s) monitor/process/filter IP addresses for enforcement purposes? If not, why? If they may, is there any special condition applicable (consent or others)?

Processing during specific litigation is allowed. Every RH has the right to process judicial data during his/her own litigation, meaning that if legal proceedings have been initiated, data may be processed for the purpose of this specific litigation.

Internet/P2P network scanning is prohibited. In-depth investigation, collection and centralization of personal data (including IP addresses) by third parties, in particular the scanning of the Internet or the request of disclosure of personal data stored by third parties (such as ISPs or controllers of Whois registers), are prohibited. Such practices fall within the competence of judicial authorities, and therefore RHs are not permitted to undertake monitoring for enforcement purposes in preparation for any future law suits.

3.2. If so, can RHs communicate the IP addresses they gathered to the ISPs for the purposes of information requests?

Communication of IP addresses to ISPs for the purpose of identifying the user is not permissible because the ISP would not be in a position to lawfully disclose the requested user data based on the IP address. An ISP would violate the obligation of telecommunications secrecy by disclosing user data. In the case of a dynamic IP address, the determination of the user's identity would violate telecommunications secrecy because it would involve the disclosure of traffic data. In the case of a static IP address, the disclosure of the data by an ISP to the RH would also violate telecommunications secrecy, because the ISP would provide information about the detailed circumstances of the telecommunication to a third party (the RH) (Section 88 Telecommunications Act, in particular Section 88 (3). A breach of telecommunications secrecy constitutes a criminal offence with the possibility of imprisonment for up to five years or a fine (Section 206 (1) Criminal Procedure Code).

4. Disclosure of the identity of Internet users (in particular of P2P users)

4.1. Can ISPs voluntarily disclose the users' details to RHs in order that they may bring a civil action? If so, under what conditions (consent, etc.)?

There is no special cooperation procedure in Germany between ISPs, RHs and DPAs. According to information from an ISP association, special cooperation procedures between ISPs, RHs and DPAs were discussed in Germany, but subsequently were abandoned because of data protection concerns. The Federal DPA came to the conclusion that the combination of traffic data with customer data in order to identify possible intellectual property right infringers is not permitted under the current data protection framework. Therefore, in order to enable a special cooperation procedure between ISPs, RHs and DPAs, an amendment of data protection law would be necessary.

ISPs may not process IP addresses to pass on infringement warning notices to users unless the data subject gives his explicit and free consent. In general, any use of an IP address must either have a statutory legal basis, or consent by the user must be received. This concerns the storage of IP addresses in log-files, linking an IP address to a particular user, and the disclosure of the data to RHs. The user must consent explicitely and freely to the relevant data processing, so that standardized consent declarations in the terms and conditions of ISPs are usually considered invalid. For consent to be valid, the user must be informed about the purposes of the processing and the categories of recipients.

Furthermore, ISPs would not be allowed to link the IP address with a particular user, and thus would not be able to deliver the infringement warning notice. In the case of a dynamic IP address, the matching of an IP address with a specific user would require examination of the log-files of the ISP, while in the case of a static IP address, it would require examining the contract with the user. In both cases, however, the use of an IP address in order to identify a particular user would constitute a use in the sense of Sections 95 and 96 Telecommunications Act, which would trigger the restrictions described above (see question 3.2) and would be considered unlawful.

ISPs may not disclose users' details to RHs in order for them to bring a civil action. Disclosure to courts and other judicial authorities of customer and traffic data for law enforcement purposes is authorized, but disclosure to private RHs for the purpose of bringing a civil action is not.

4.2. Is there any procedure in place to compel ISPs to disclose the identity of Internet users suspected of online copyright infringement within the framework of (1) criminal enforcement by judicial authorities or (2) civil enforcement by RHs?

There is no procedure in place that compels ISPs to disclose the identity of P2P users, except in cases where the ISP receives a judicial order issued by a law enforcement authority or a court to disclose the data.

ANNEX

Interpretation of the term "commercial scale" by German courts according to Section 101 of the Copyright Act, under which RHs may bring a claim to request disclosure of the identity of users (see section 2.3)

Note: This list is illustrative, and is not intended to be exhaustive.

No.	Court	"Commercial scale" as interpreted by the courts	Comments
1	OLG Karlsruhe, Beschluss v. September 1, 2009 (Az. 6 W 47/09)	For example a complete movie file, a music album or audio book that is illegally made available before of directly after publication in Germany to an undefined number of third parties.	
2	LG Köln, Beschluss v. April 30, 2009 (Az. 9 OH 388/09)	The making available of a protected work via file-sharing as such does not suffice for determining "commercial scale".	
3	LG Köln, Beschluss v. December 17, 2008 (Az. 38 OH 11/08)	The publication of a single audio book in a file sharing system. In case the audio book was not uploaded on the Internet directly before or after the publication, "commercial scale" exists if the audio book continues to be listed high in the charts and continued exploitation is planned.	
4	OLG Oldenburg, Beschluss v. 1.12.2008 (Az. 1 W76/08)	A single album is insufficient.	
5	OLG Zweibrücken, Beschluss v. October 27, 2008 (Az. 3 W 184/08)	Not commercial scale if just a three-month-old computer game, except if the game is a product that is well-positioned in the	

		market.	
6	LG Nürnberg (Az.: 3 O 8013/08), September 22, 2008	1 music album file or audio book	
7	LG Frankfurt am Main (Az.: 2-06 O 534/08), September 18, 2008	1 music album file or audio book	
9	LG Bielefeld (Az.: 4 O 328/08), September, 2008	1 music album file or audio book	
10	LG Oldenburg (Az.: 5 O 2421/08), September 15, 2008	1 music album file or audio book	The simple use of a P2P network was considered to be an indication that the user was not acting for private purposes.
11	LG Frankenthal (AZ.: 6 O 325/08), September 15, 2008	3000 song files or 200 movie files	Similar to the public prosecutor guidelines developed in various federal states on the conditions under which prosecution for file-sharing should be initiated.
12	LG Düsseldorf (Az.: 12 O 425/08), September 12, 2008	1 music album file	
13	LG Köln (28 AR 4/08), September 2, 2008	1 music album file	

E. Spain

Prepared by:
Javier Aparicio Salom
Cuatrecasas, Gonçalves Pereira
Madrid, Spain

Table of legislation

Denomination	Reference
AEPD	Spanish Data Protection Agency (Agencia Española de Protección de Datos)
Data Protection Act	Organic Act 15/1999 of 13th December 1999 on Personal Data Protection
E-Commerce Act	Act 34/2002, of July 11, 2002 on services of the information society and electronic commerce
Data Retention Act	Act 25/2007 of October 18 2007 on conservation of data concerning electronic communications and public communications networks

1. Nature of an IP address

1.1. Is an IP address considered to be personal data/traffic data? (Please consider temporary and permanent IP addresses and explain your reasoning.)

An IP address is personal data (Article 3 a) Data Protection Act). This has been confirmed several times by the Spanish DPA (the AEPD): Report 327/2003 on the nature of IP addresses as personal data, Report 213/2004 on disclosure of IP addresses to law enforcement agencies, etc. Since an IP address is considered to be personal data, data protection law applies.

However, in its judgment no. 236/2008 dated May 9, 2008, Section 1 of the criminal division (*Sala de lo Penal*), the Spanish Supreme Court stated that IP addresses circulating on P2P networks are not protected by the right to privacy, and judicial authorization is not necessary to obtain what is in the public domain, since the network user himself was the one who placed this information on the network. Anyone using a P2P program assumes that most of the data will become public for Internet users.

An IP address is also traffic data. Under Article 5 of Act 25/2007 of October 18, 2007 on Data Retention (*Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones*), which implements the Data Retention Directive, telecommunications service providers (including ISPs) have a duty to withhold data on traffic and location, in addition to any related data necessary to identify the

subscriber or registered user, for a maximum of twelve months.[25] Telecommunications secrecy continues to apply to stored data.

Note that traffic data must be kept by telecommunications operators "for the purposes of detection, investigation and prosecution of serious criminal offences" (Article 1.1 Data Retention Act). Article 3 Data Retention Act determines the categories of data that must be kept, depending on the service provided.

In addition, the recent Royal Decree 1720/2007 of December 21, 2007, amending the Spanish Data Protection Act of 1999, is also applicable. According to this new Decree, operators who provide electronic communications services processing traffic and location data must apply special security measures.

1.2. Is an IP address related to a user committing or facilitating copyright infringement considered to be sensitive data, i.e., judicial data? If so, what is the legal basis for this conclusion and does that regime imply any restrictions, e.g., processing only with consent of the user?

An IP address related to a user committing or facilitating copyright infringement is not considered to be judicial data (i.e., sensitive data), and its processing does not require specific consent. Only personal data disclosing the ideology, trade union membership, religion and beliefs, as well as referring to racial origin, health and sex life are considered to be sensitive data (Article 7 Data Protection Act) and require specific consent by the data subject.

However, under the Data Protection Act, only the administrative authorities can create databases to process information related to criminal records and infringements.

2. Processing and retention of IP addresses by ISPs

2.1. Can an ISP store IP addresses and subscribers' details when those data are no longer needed for the purposes of the transmission of the communication? If so, can the ISP keep the data for the purpose of fighting online copyright infringement? If applicable, please differentiate between (1) criminal enforcement by judicial authorities and (2) civil enforcement by right holders (RHs)?

Under Article 1 Data Retention Act, which implements the Data Retention Directive, ISPs must retain traffic and location data and any related data necessary for identifying the subscriber or registered user.

ISPs must keep data for one year from the date of the communication for the purposes of investigation, detection and prosecution of serious criminal offences (delitos graves) (Article 5 Data Retention Act). Extraordinarily, and in line with the regulations (to be adopted), the retention period can be extended to a maximum of two years or reduced to a minimum of six

[25] Article 12 e-Commerce Act was revoked by the Data Retention Act, that substitutes the regulation on data retention.

months after consulting with ISPs and taking into consideration the cost of storing and keeping the data, as well as the significance of the data for these purposes.

When the retention period ends, according to Article 16 of the Spanish Data Protection Act (*Ley Orgánica de Protección de Datos*), the ISP must "cancel" any personal data (for example, the IP address or any other type of information that identifies or enables identification of an individual). Cancellation means that the ISP must block and maintain those data exclusively for use by the public administration, judges and courts to determine any liability arising from the processing for the duration of this liability. When this liability expires, the ISP must delete the data.

However, under Article 1 Data Retention Act, ISPs can only keep the data to disclose them to the relevant authorities for the purposes of investigation, detection and prosecution of serious criminal offences. The Spanish Criminal Code (Código Penal) states that serious criminal offences are acts punished by a prison sentence greater than five years (or other specific sanctions). This means that data cannot be disclosed for criminal offences punished by a lower prison sentence (which is the case of criminal offences linked to intellectual property rights), or for civil infringements.

ISPs cannot retain any data revealing the content of the communications (Article 3.2 of Act 25/2007 and Article 5.2 Data Retention Directive).

2.2. Can ISPs process IP addresses to pass on infringement warning notices to users? If so, under what conditions (consent, etc.)?

Processing IP addresses to pass on infringement warning notices to users is prohibited unless the ISP obtains the consent of the data subjects.

Communication of infringement warning notices to users constitutes data disclosure. Data disclosure is regulated by Article 11 Data Protection Act. The Data Protection Act does not allow data disclosure to initiate a civil action, nor does the e-Commerce Act, unless the ISP obtains the consent of the data subjects. For consent to be valid, the data subject must be informed of the purpose of the disclosure and of the person to whom the data will be disclosed. Consent can be revoked. In practice, consent is nevertheless very difficult to use as a legal basis.

In addition, this would violate the Data Retention Act, since personal data retained under this Act can only be processed for limited purposes, which do not include disclosing data to RHs to enable them to warn Internet users**.**

3. Monitoring of the Internet (in particular of P2P networks)

3.1. Can RHs or their representative(s) monitor/process/filter IP addresses for enforcement purposes? If not, why? If they may, is there any special condition applicable (consent or others)?

RHs are not entitled to monitor IP addresses for enforcement purposes. Monitoring means gathering information related to an IP address and activity on the Internet, and then processing it. Processing of IP addresses is only possible under the conditions established in Article 6 of the

Data Protection Act. Since an IP address is considered to be personal data, the general regime that regulates data processing applies. Therefore, Article 6 (consent of the data subject) of the Data Protection Act applies, but cannot serve as a legal basis to legitimize the processing, because it is always possible to revoke consent. Note that, in the past, the DPA has allowed the disclosure of IP addresses, but only in cases limited to disclosure to law enforcement agencies, when the party reporting was the actual operator and the case related to criminal behavior, or when the law expressly obliged individuals to cooperate with law enforcement agencies (e.g., bank secrecy or cooperation with the tax authorities).

3.2. If so, can RHs communicate the IP addresses they gathered to the ISPs for the purposes of information requests?

RHs may not communicate IP addresses to the ISPs for the purpose of establishing the identity of the users or asking the ISP to identify users to send them any communication.

4. Disclosure of the identity of Internet users (in particular of P2P users)

4.1. Can ISPs voluntarily disclose the users' details to RHs in order that they may bring a civil action? If so, under what conditions (consent, etc.)?

ISPs cannot voluntarily disclose the users' details to RHs in order that they may bring a civil action. Data disclosure is regulated by Article 11 of the Data Protection Act. The Data Protection Act does not allow data disclosure to initiate a civil action, nor does the e-Commerce Act. In addition, there is no special cooperation procedure between ISPs, RHs and the DPA in Spain.

4.2. Is there any procedure in place to compel ISPs to disclose the identity of Internet users suspected of online copyright infringement within the framework of (1) criminal enforcement by judicial authorities or (2) civil enforcement by RHs?

(1) Criminal enforcement

Given that criminal enforcement by judicial authorities tends to be based on the proportionality principle applied to the balancing of the rights in conflict, the criminal courts usually ask third parties to cooperate to help them detect and investigate criminal offences by providing information that can include the identity of the persons related to the investigation. Under the Criminal Proceedings Act (*Ley de Enjuiciamiento Criminal*), individuals must cooperate with the judicial authorities. In case of non-cooperation, ISPs will be held liable and may face sanctions.

However, this cooperation should limit the information to what is necessary to detect, investigate and prosecute serious criminal offences, as the obligation to retain data limits the purposes for which the data may be used to these cases. To use the data for other purposes, these would need to be established by law.

(2) Civil enforcement

There is no procedure in place that compels ISPs to disclose the identity of P2P users within the framework of civil enforcement by RHs. The principle of proportionality has probably prevented

the method usually used in criminal proceedings from taking effect; in any event, we are not aware of any precedents in civil proceedings in which a judicial authority requested ISPs to cooperate and to identify a user.

Regarding civil enforcement by judicial authorities, this issue has been the focus of a case which led to the ECJ Promusicae case. The Commercial Court No. 5 of Madrid asked the European Court of Justice (ECJ) for a preliminary ruling on whether Spanish law, which prohibits the disclosure of the identity of P2P users within the framework of civil enforcement by RHs, was compliant with European law.

On January 29, 2008, the ECJ held that the e-Commerce Directive, the Copyright in the Information Society Directive, the IP Enforcement Directive, and the e-Privacy Directive "do not require the Member States to lay down 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. Furthermore, 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 general principles of Community law, such as the principle of proportionality."

There has not yet been any official reaction by the Spanish government following the judgment of the ECJ. As it was handed down as a preliminary ruling under Article 234 of the EC Treaty, it has immediate effect in the specific case. The judgment does not challenge the conformity of Spanish law with Community law.

The Data Retention Directive was implemented in Spain by the Data Retention Act 2007 (before the ECJ's judgment, but probably considering the preliminary ruling requested by the Commercial Court). As the Data Retention Act limits the use of the data to detect, investigate and prosecute serious criminal offences, any extension of these purposes is illegal unless it is embedded in a law that modifies or excepts this limitation. Consequently, the possibility of forcing ISPs to disclose the identity of Internet users suspected of online copyright infringement within the framework of civil enforcement by RHs in Spain is limited by law.

Following the ECJ's judgment, the Commercial Court No. 5 of Madrid ruled on March 17, 2008, that Article 12.2 LSSI (derogated by the Data Retention Act) permitted the data retained to be used for purposes other than those provided for in paragraph 3 of this article (criminal investigation, public security and national defense), emphasizing that Article 12.2 LSSI only allows alternative use when expressly authorized by law. The Court declared that Articles 11.2 Data Protection Act and 29 Minor Commerce Act do not contain any obligation to disclose personal information in the context of civil enforcement (it recognized that under Article 11.2 Data Protection Act, consent does not need to be given when data are disclosed to judges or courts for legal reasons), but declared that "this case has nothing in common with the purposes for which the data may be used and that must be authorized by law". Thus, the Court interprets this article as limiting the purposes and declares the need for a new law to establish an exception

to the limitation, adding new or different purposes. Consequently, the Commercial Court No. 5 of Madrid held that Telefónica's opposition is based on law and that it does not have any obligation to provide the information requested.

Finally, it seems that the upcoming Spanish presidency of the European Union in 2010 has the fight against online piracy on its agenda, and will try to tackle this issue at a political level by reviewing the applicable Spanish legal framework.

F. Sweden

Prepared by:
Ann-Charlotte Högberg
Mannheimer Swartling Advokatbyrå
Stockholm, Sweden

Table of legislation

Denomination	Reference
Copyright Act	Act on Copyright to Literary and Artistic Works (1960:729)
DPA	Datainspektionen (Data Inspection Board)
Data Protection Act	Data Protection Act (1998:204)
DIFS 1998:3	Data Inspection Board Statute Book (1998:3)
Electronic Communications Act	Electronic Communications Act (2003:389)

1. Nature of an IP address

1.1. Is an IP address considered to be personal data/traffic data? (Please consider temporary and permanent IP addresses and explain your reasoning.)

An IP address is personal data. Personal data are, according to the broad definition in Section 3 of the Data Protection Act (1998:204), "all types of information that directly or indirectly may be referable to a natural person who is alive."

The DPA has confirmed this position on more than one occasion, one of which concerned the processing by the Swedish Anti-Piracy Bureau[26] of IP addresses in the context of investigating cases of alleged copyright infringement, where the DPA concluded, with reference to recital 26 of the Directive 95/46/EC, that an IP address is to be deemed as personal data where someone, *e.g.,* an ISP, has access to information that may be used to link an IP address to an individual. Accordingly, in respect of IP addresses that are under processing, the requirements of the Data Protection Act must be complied with. The DPA's decision was appealed by the Anti-Piracy Bureau first to the County Administrative Court, which confirmed the DPA's position, and then to the Administrative Court of Appeal, which also confirmed the DPA's position in its judgment (case number 285-07) issued in 2007. According to the Administrative Court of Appeal, IP addresses are considered to be personal data when they can be traced back to natural persons. To

[26] The Anti-Piracy Bureau *(Antipiratbyrån)* was established in 2001 by three film and music groups (Filmägarnas Kontrollbyrå, MDTS, and Sveriges Videodistributörers Förening) and represents a Swedish lobbying group that collects and processes IP addresses for the purpose of investigating cases of alleged copyright infringement.

support this, the Court invoked Article 2(a) of Directive 95/46/EC. Where IP addresses are linked to an individual through information that is stored by an ISP, they can be used to identify an Internet subscriber. Consequently, regardless of whether the actual user can be identified, an IP address can reveal an identifiable natural person, namely the Internet user/subscriber. The judgment of the Administrative Court of Appeal was appealed by the Anti-Piracy Bureau, but the Supreme Administrative Court of Appeal resolved in June 2009 not to grant leave of appeal and, accordingly, confirmed this position.

An IP address is traffic data. According to Chapter 6, Section 1 of the Electronic Communications Act (2003:389), traffic data are data that are processed for the purpose of forwarding an electronic message via an electronic communications network or of invoicing such service. Accordingly, an IP address (at least when public) will in many instances also be deemed to be traffic data.

1.2. Is an IP address related to a user committing or facilitating copyright infringement considered to be sensitive data, i.e., judicial data? If so, what is the legal basis for this conclusion and does that regime imply any restrictions, e.g., processing only with consent of the user?

An IP address processed in the context of alleged copyright infringement is judicial data. The DPA has taken the position that processing of an IP address in the context of alleged copyright infringement is to be deemed to constitute the processing of judicial data. This position has won general acceptance and is supported by statements made in the legislative history of recent amendments to the Act on Copyright to Literary and Artistic Works (1960:729).[27]

According to Section 21 of the Data Protection Act (1998:204), it is prohibited for parties other than public authorities to process personal data concerning legal offences involving crime, judgments in criminal cases, coercive criminal procedural measures or administrative deprivation of liberty. It is stated in the legislative history that information on an individual who has or may have committed a crime is deemed to be judicial data, even in the absence of a conviction. Processing that relates only to a single item of information that is necessary to determine, enforce or defend claims in individual cases has been exempted through a block exemption (DIFS, 1998:3). The Government or the DPA may also grant exemptions in individual cases. The prohibition may not, however, be lifted with the data subject's consent.

The DPA has granted several individual exemptions from Section 21 of the Data Protection Act (1998:204), including for purposes of identifying suspected copyright infringement (granted to the Anti-Piracy Bureau and IFPI). However, on April 1, 2009, amendments (based on the IP Rights Enforcement Directive (2004/48/EG)) to the Copyright Act entered into force, pursuant to which, by derogation from Section 21 of the Data Protection Act, personal data may be processed in the context of alleged copyright infringements if this is necessary to determine, enforce or defend legal claims.

[27] See further below in this section.

2. Processing and retention of IP addresses by ISPs

2.1. Can an ISP store IP addresses and subscribers' details when those data are no longer needed for the purposes of the transmission of the communication?

In general, no. Pursuant to the Electronic Communications Act (2003:389), Chapter 6 Section 5, traffic data concerning users that are individuals or subscribers must be erased or anonymized at the time when they are no longer necessary for the transmission of an electronic message, except:

(a) where the traffic data are required for the purposes of invoicing, they may be processed until the invoice has been paid or the possibility to raise objections to the invoice time-barred;
(b) subject to the individual's consent, they may be processed for purposes of marketing value-added services; and
(c) for certain purposes and subject to certain requirements, the restriction on the disclosure of the caller's identity and associated location data may be circumvented in emergency situations or upon request of a subscriber.

2.2. If so, can the ISP keep those data for the purpose of fighting online copyright infringement? If applicable, please differentiate between (1) criminal enforcement by judicial authorities and (2) civil enforcement by right holders (RHs)?

No, an ISP cannot generally keep IP addresses only for the purpose of fighting online copyright infringement since this is not included in the list of exceptions of the Electronic Communications Act (2003:389), Chapter 6 Section 5 (see above under 2.1), unless ordered by a court in a specific case to do so. In this context, it may be noted that Sweden has not, as yet, implemented Directive 2006/24/EC.

Pursuant to the Electronic Communications Act (2003:389), Chapter 6 Section 8, the obligation to erase or anonymize traffic data does not apply:

(a) when a governmental authority or court of law needs access to traffic data for the purposes of dispute resolution;
(b) for electronic communications which are transmitted or have been dispatched to or from a certain address in an electronic communications network which is subject to a decision on secret wiretapping or secret interception of telephone calls, or technical aid for such purposes; or
(c) to the extent that traffic data are necessary for the prevention or detection of unauthorized use of a telecommunications network or service.

The data may not be retained for a period longer than what is necessary for the purposes of the processing. Further to statements made in the legislative history, retention periods exceeding a year are generally not acceptable, except in certain circumstances, *e.g.,* if a dispute has arisen, or a preliminary investigation has been initiated.

2.3. Can ISPs process IP addresses to pass on infringement warning notices to users? If so, under what conditions (consent, etc.)?

ISPs are considered to be able to forward an infringement warning notice to users under certain conditions:

(a) where a service for electronic conveyance of messages (covering, *e.g.,* so called electronic bulletin boards but also other services through which users can send and receive messages) is concerned, if it is obvious that the user has committed a copyright infringement (in which case the ISP is under an obligation to take down or otherwise prevent further infringement pursuant to the Act on Electronic Bulletin Boards (1998:112);

(b) supported by the terms of their agreements with users (although this possibility is in practice limited, due to Section 21 of the Data Protection Act and subject to DIFS 1998:3, see item 1.2 above).

3. Monitoring of the Internet (in particular of P2P networks)

3.1. Can RHs or their representative(s) monitor/process/filter IP addresses for enforcement purposes? If not, why? If they may, is there any special condition applicable (consent or others)?

Further to Chapter 7 Section 53g of the Copyright Act, which entered into force on April 1, 2009, personal data may be processed in the context of alleged copyright infringements if this is necessary for establishing, making or defending legal claims. The information may be used to take action to prevent further infringement, such as contacting the subscriber or initiating proceedings against it, but may not be used for purposes of keeping a database or registry about Internet users who are suspected of file-sharing or other types of copyright infringement.

Consent is not a valid legal basis for the processing of judicial data.

Pursuant to Chapter 6 Section 5 of the Electronic Communications Act, ISPs may process traffic data for purposes of message transmission and billing and under certain exceptional circumstances of no relevance here, but not in any other case, and the data may not be retained after those purposes have been achieved.

3.2. Can RHs communicate the IP addresses they gathered to the ISPs for the purposes of information requests?

RHs may process IP addresses in very limited circumstances (for establishing, making or defending legal claims), but those circumstances do not include the communication to the ISPs for the purposes of information request. As mentioned above, since IP addresses in the context of alleged copyright infringements are deemed to be judicial data, they may – in the absence of an individual exemption permitting this having been granted as set forth above under item 1.2 - be processed only if this is necessary for establishing, making or defending legal claims. Since an ISP may not disclose user details based on the IP addresses unless compelled to do so under the circumstances highlighted below under 4.2, it is questionable whether RHs can commmunicate

those details to ISPs, as it would serve no purpose and, accordingly, would not seem to be necessary for establishing, making or defending legal claims.

4. Disclosure of the identity of Internet users (in particular of P2P users)

4.1. Can ISPs voluntary disclose the users' details to RHs in order that they may bring a civil action? If so, under what conditions (consent, etc.)?

No, ISPs are subject to the confidentiality regime of the Electronic Communications Act and may only disclose their users' details in accordance with what is set forth therein.

4.2. Is there any procedure in place to compel ISPs to disclose the identity of Internet users suspected of online copyright infringement within the framework of (1) criminal enforcement by judicial authorities or (2) civil enforcement by RHs?

(1) Criminal enforcement by judicial authorities

Traffic data and subscriber data may also be disclosed to police or law enforcement agencies upon their request pursuant to Chapter 6 Section 22 of the Electronic Communications Act, entailing that an ISP may disclose subscriber information upon suspicion of a criminal offence for which imprisonment is a potential sanction and the police or law enforcement authority considers that the crime may result in a sanction other than a fine.

An ISP is also obligated to produce documents as evidence pursuant to Chapter 38 Section 2 of the Code of Judicial Procedure (1942:740) or in the context of witness examination pursuant to Chapter 36 Section 1 of the Code of Judicial Procedure. This entails that the proceedings have been initiated and would therefore require that the suspect has already been identified.

(2) Civil enforcement by RHs

Upon application of a RH or licensee, a court may issue a conditional fine order to an ISP to provide information on the origin of the infringing products or services or of the distribution network.[28] The conditional fine order may be issued only if: (1) the applicant can show probable grounds that an infringement has been committed; and (2) the information can be assumed to facilitate investigation of the infringement. Also, an order to provide information may be granted only if the purposes outweigh the inconvenience or harm that the measure would cause the party against which it is directed or any opposing interest (proportionality test).[29]

This recent piece of legislation has already been subject to the scrutiny of the Swedish courts (Solna District Court, Case No. Ä 2707-09, Svea Court of Appeal, Case No. ÖÄ 6091-09):

In the first instance, the Solna District Court ordered an ISP to provide audio book publishers with the name and address of the user of an IP address identifying an FTP server on which the

[28] See Chapter 7 Section 53c of the Copyright Act, that entered into force on April 1, 2009.

[29] Chapter 7 Section 53d of the Copyright Act.

relevant works were stored, subject to a non-compliance penalty of SEK 750,000. The Solna District Court first noted that there was a potential conflict between the RH's right to information and the user's fundamental right to privacy. The Court referred to the ECJ Promusicae case (C-275/06) regarding the need to achieve a balance between the right of information and the protection of privacy.

The Solna District Court noted that Directive 2002/58/EC imposes derogations from the duty of confidentiality, in particular when it is necessary to protect any other person's rights and freedoms. The Solna District Court found that the evidence supported the fact that a large amount of audio books were stored on the server, and that this itself constituted grounds for assuming that the books had been made available to the public (although login details were required to access the server and there was no evidence presented as to how many users had access to those login details).

The Solna District Court referred to the legislative history, which mentions that the infringement must be of a certain scale, and that this requirement would usually be met if the infringement concerned the making available of a work to the public or if extensive downloading of works was involved. Since the works were available on the Internet, the Court considered that it was most likely that there had been an extensive copyright infringement. In addition, the Court considered that subscribers would not suffer any major inconvenience by being subjected to the investigation of copyright infringement at stake. Accordingly, the Court found that it would be proportionate to issue the order. The ISP appealed this decision to the Svea Court of Appeal.

The Svea Court of Appeal issued its judgment on October 13, 2009. The Court of Appeal held that the European Convention on Human Rights does not generally prevent the disclosure of a subscriber's identity, but that the ECJ in the Promusicae case had concluded that the provisions of the Copyright Act must be construed in the light of the various fundamental rights referred to therein. Accordingly, in the present case, the principles of right to privacy, law and order, and proportionality must be given particular weight. The Court concluded that RHs had presented some evidence supporting the fact that the library of audio books made available on the FTP server was extensive. This fact clearly indicates that more than just a few individuals would have had access to the server and, accordingly, that the audio books would have been communicated to the public.

However, no evidence was presented regarding how the RHs had accessed the login details or if anyone other than the RHs had been able to download works. Therefore, the Court found, it was impossible to render a judgment as to the amount of people who had access to the server, the purpose of the server, terms of entry, or whether there was any purpose of profitability behind the server. In conclusion, the Svea Court of Appeal found that the RHs had not presented evidence of probable grounds, and reversed the order of the Solna District Court, with two judges dissenting. The judgment has been appealed to the Supreme Court.

Also in the context of civil enforcement, the obligations to produce documents as evidence or provide information in the context of witness examination apply. However, those obligations will not apply if the counterparty has not already been identified. Under certain circumstances, the procedure for taking of evidence in anticipation of an upcoming trial (Chapter 41 Section 1 of the Code of Judicial Procedure) may also be used, although since the purpose of this procedure is to

secure evidence of already known facts, it cannot be used for purposes of identifying an unknown individual.

The views expressed are those of the authors and do not necessarily express the views of the European Commission.