Private Peers –

What Role Should Privacy Law Play

in Learning the Identities of P2P Users?

The European Case

By Dr. Volker KITZ, LL.M. (New York University)[*]

Sixteenth Annual Conference on

Intellectual Property Law & Policy

Fordham Intellectual Property Law Institute

March 27 and 28, 2008

Last revised on: March 19, 2008

[*] © 2008 Dr. VOLKER KITZ,

- Senior Research Fellow, Max Planck Institute for Intellectual Property, Competition and Tax Law, Munich, Germany;
- Attorney at Law, HOECKER, Cologne, Germany.
- Dr. iur., University of Cologne, 2004; LL.M., New York University, 2002; J.D., University of Cologne, 2000.
- The author can be reached at kitz@hoecker.eu .

Contents

I. From IP Address to IP Enforcement 2
A. Storage of IP Addresses 4
B. Obligation to Disclose User Identity 7
C. Permission Under Privacy Law to Use IP Addresses for Disclosure 8
II. Can the "No, No, Never" Approach Strike the Right Balance? 11
III. Can the "Provider Does It All" Approach Strike the Right Balance? 13
IV. Proposal for a Two-Tiered System 15

I. From IP Address to IP Enforcement

Tracing down individual peer-to peer (P2P) users who infringe copyrights can be a tough game. In most cases, a right holder does not have more than a screen name and an IP address. The screen name will not get the right holder very far: P2P users do not use their real names as screen names, and a screen name like tereastarr@KaZaA[1] is not a name one can easily take to court.

The IP address is oftentimes a dynamic one: It is allocated to the Internet user only for a limited online session. If a right holder wants to know the name of the user who was allocated a certain IP address at a certain time, e.g., when the user was offering a protected work for download on a P2P file sharing system, he needs to get this information from someone who keeps track of the IP addresses allocated over time.

[1] As used by the defendant in Capitol Records Inc., et al. v. Jammie Thomas, No. 06-cv-1497 (D. Minn. 2007).

This might be the access provider of the user because the access provider allocates IP addresses to users. But the way from IP address to IP enforcement can be burdensome in Europe. To learn the identity of an Internet user from his dynamic IP address, three preconditions must be fulfilled:

1. The dynamic IP address and the matching user name must have been stored by the access provider and not yet been erased. If the data do not exist, a right holder will never be able to get them, no matter how nicely he asks or how well he litigates.

2. The access provider must be legally obliged to disclose the data to the right holder. The access provider has, like anyone doing business, an interest in protecting his customers' privacy. Only a legal obligation to disclose the information will help the right holder in court.

3. Finally, and this is a point European right holders had to learn the hard way: Privacy law must not prohibit the disclosure of the data. As recent European case law shows,[2] even if the data exist and if the provider has a legal obligation do disclose the information to the right holder, privacy law can still be in the way.

[2] See *infra*, I C.

A. Storage of IP Addresses

Until recently, the legal way[3] to obtain the identity of a user in exchange for a dynamic IP address was bound to fail because not even the first of these three preconditions was fulfilled: There were no data stored. Under Art. 6 of the Directive on Privacy and Electronic Communications,[4] traffic data[5] had, in principal,[6] to be erased or made anonymous when they were no longer needed for the purpose of the transmission of a communication or for the purpose of subscriber billing and interconnection payments. And with the advent of flat rates for Internet access, dynamic IP addresses had generally lost their relevance for subscriber billing services. As a

[3] Some access providers used to store dynamic IP addresses without a legal basis. These data were even used by criminal prosecution officials, see Volker Kitz, *Die Auskunftspflicht des Zugangsvermittlers bei Urheberrechtsverletzungen durch seine Nutzer*, 12 Gewerblicher Rechtsschutz und Urheberrecht [GRUR] 1015 (2003).

[4] Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, 2002 O.J. (L 201) 37.

[5] Traffic data is defined in Art. 2 (b) of Directive 2002/58/EC as "any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof".

[6] With the user's consent, the traffic data may, under Art. 6 (3) of Directive 2002/58/EC, also be used for the purpose of marketing electronic communications services or for the provision of value added services.

consequence, under the old regime, a dynamic IP address had to be erased immediately upon the termination of the Internet connection. [7]

However, the European legislator decided a 180-degree-turnaround: The so called Data Retention Directive[8] was passed. Its objective is to combat "serious crime".[9] The term „serious crime" is to be defined "by each Member State in its national law". The German legislator, e.g., generally classified, *inter alia*, crimes committed by means of telecommunications as serious.[10] The original proposal of the European Commission had, much more narrowly, focused on organized crime and terrorism to justify the legislative action;[11] but these narrow justifications are, in the final version

[7] See for Germany BGH (German Supreme Civil and Criminal Court), 1 Multimedia und Recht [MMR] 37 (2007).

[8] Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, 2006 O.J. (L 372) 32.

[9] Art. 1 of Directive 2006/24/EC.

[10] See § 100g (1) German Rules of Criminal Procedure (Strafprozessordnung – StPO), BGBl. I 2614 (2007). In a preliminary judgment, the German Federal Constitutional Court has already restricted the application of the new law, see *infra*, footnote 23.

[11] See Francesca Bignami, *Privacy and Law Enforcement in the European Union: The Data Retention Directive*, 8 Chi. J. Int'l L. 233 (2007).

of the Directive, only referred to incidentally.[12] The Directive had to be transposed in Member States by September 15, 2007.[13]

Basically, the new law obliges communication service providers to store the following information: Who communicated with whom, when, how long, and from where? Data must be stored and kept available for at least six months, but no longer than two years from the date of the communication.[14] Art. 5 of the Directive specifies the categories of data to be stored and explicitly refers to IP addresses.[15] As a result, a record of IP addresses allocated to users at a certain point in time now generally exists with European access providers, at least for a limited period of time.

[12] See recitals 8 and 9 of Directive 2006/24/EC.

[13] See Art. 15 of Directive 2006/24/EC; however, Member States could declare upon adoption of the Directive to postpone the application of the Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail until March 15, 2009. Several Member States made this reservation.

[14] See Art. 6 of Directive 2006/24/EC.

[15] See Art. 5 (2) (c) (2) (i) of Directive 2006/24/EC: „the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet access service provider to a communication, and the user ID of the subscriber or registered user".

B. Obligation to Disclose User Identity

Also fulfilled is the second precondition for the right holder to obtain the information he needs: Art. 8 (1) of the IP Enforcement Directive[16] obliges the Member States to ensure that, in the context of proceedings concerning an infringement of an intellectual property right, courts may order that information about the identity of the infringer be provided by any person who, *inter alia*, provides on a commercial scale services used in infringing activities.[17] This aims at access providers who would, under this rule, have to disclose to right holders the identity of infringing users.

[16] Directive 2004/48/EC of the European Parliament and of the Council on the enforcement of intellectual property rights, 2004 O.J. (L 195) 16.

[17] Art. 8 (1) of Directive 2004/48/EC reads: "Right of information – 1. Member States shall ensure that, in the context of proceedings concerning an infringement of an intellectual property right and in response to a justified and proportionate request of the claimant, the competent judicial authorities may order that information on the origin and distribution networks of the goods or services which infringe an intellectual property right be provided by the infringer and/or any other person who: (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."

C. Permission Under Privacy Law to Use IP Addresses for Disclosure

However, the European Court of Justice (E.C.J.) now decided, in a preliminary ruling under Art. 234 EC, that Art. 8 (1) of the IP Enforcement Directive does not suffice to force access providers to disclose the identity of an infringing user.[18] The reason is Art. 8 (3) (e) of the same Directive which declares that the obligation to provide information is without prejudice to other statutory provisions which govern the protection of confidentiality of information sources or the processing of personal data. In other words: If IP enforcement law says "You must disclose the data" and, at the same time, privacy law says "You must not disclose the data", privacy law will prevail in this conflict. For the right holder's right to information to work effectively, privacy law must explicitly *allow* the use of the data necessary to provide the information owed under the IP Enforcement Directive. Otherwise privacy law will render ineffective the obligation to disclose information laid down in Art. 8 (1) of the IP Enforcement Directive.

In the case before the E.C.J., Spanish law[19] provided that the IP addresses could not be used for purposes other than criminal investigation or

---

[18] E.C.J., No. C-275/06, Promusicae v. Telefónica, of January 29, 2008. The Austrian Supreme Court brought a similar case before the E.C.J. which is still pending, see Oberster Gerichtshof, No. 4 Ob 141/07z.

[19] Article 12 of Law 34/2002 on information society services and electronic commerce (Ley 34/2002 de servicios de la sociedad de la información y de comercio electrónico) of 11 July 2002 (BOE No 166 of 12 July 2002,

safeguarding public security and national defense. As a consequence, the access provider, Telefónica, did not have to – or more precisely: was not even allowed to – use the IP address in order to provide information for civil proceedings.

The E.C.J. decided that privacy law prevailed over IP enforcement law in this case. The E.C.J. also decided – and this is the more important point –

---

p. 25388, 'the LSSI'), headed 'Duty to retain traffic data relating to electronic communications' reads:

"1. Operators of electronic communications networks and services, providers of access to telecommunications networks and providers of data storage services must retain for a maximum of 12 months the connection and traffic data generated by the communications established during the supply of an information society service, under the conditions established in this article and the regulations implementing it.

2. … The operators of electronic communications networks and services and the service providers to which this article refers may not use the data retained for purposes other than those indicated in the paragraph below or other purposes permitted by the Law and must adopt appropriate security measures to avoid the loss or alteration of the data and unauthorized access to the data.

3. The data shall be retained for use in the context of a criminal investigation or to safeguard public security and national defense, and shall be made available to the courts or the public prosecutor at their request. Communication of the data to the forces of order shall be effected in accordance with the provisions of the rules on personal data protection."

that a Member State does not even *have* to match its privacy law with IP enforcement law to make the latter work on the Internet. On the other hand, the E.C.J. found that privacy law does not *hinder* a Member State to make IP addresses available for civil proceedings in copyright infringement cases. To find this, the E.C.J. looked a bit more deeply into the complex European privacy law: Art. 15 (1) of the Directive on Privacy and Electronic Communications[20] refers to Art. 13 (1) of the Data Protection Directive.[21] And Art. 13 (1) (g) of the Data Protection Directive provides that Member States "may" adopt legislative measures to restrict the scope of data protection to safeguard, *inter alia*, "the rights and freedoms of others". An intellectual property right, the E.C.J. found, can be such a right. And "may" means "may" – not "must", and not "must not". In other words: It lies within a relatively broad discretion of each Member State to strike a fair balance between IP protection and privacy.

[20] Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, 2002 OJ (L 201) 37.

[21] Directive 95/46/EC 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, 1995 O.J. (L 281) 31.

II. Can the "No, No, Never" Approach Strike the Right Balance?

Spain[22] and other Member States, e.g. Germany[23] and Austria[24], have struck this balance completely in favor of privacy: Dynamic IP addresses must generally not be used for private law enforcement.

The main reason for this political decision in Germany, e.g., was a strong public pressure to restrict the use of the communication data retained under the new data retention obligation. The data retention obligation has been highly controversial and is currently subject to more than 30,000 constitutional challenges.[25] Facing strong public protest already,[26] the

[22] Article 12 of Law 34/2002 on information society services and electronic commerce (Ley 34/2002 de servicios de la sociedad de la información y de comercio electrónico) of 11 July 2002 (BOE No 166 of 12 July 2002, p. 25388, 'the LSSI').

[23] § 113 b German Telecommunications Act (Telekommunikationsgesetz – TKG), BGBl. I 3198 (2007). Just last week, on March 19, 2008, the German Federal Constitutional Court even decided in a summary judgment that the data may not be used for the general purpose of criminal prosecution, but only for the prosecution of a defined list of very serious crimes, see BVerfG, No. 1 BvR 256/08.

[24] § 99 Austrian Telecommunications Act (Telekommunikationsgesetz – TKG), BGBl. I 983 (2003).

[25] See Verfassungsbeschwerde (constitutional complaint) of December 31, 2007, 1 BvR 256/08. In a preliminary judgment, the German Federal Constitutional Court has already restricted the application of the new law, see *supra*, footnote 23. Apart from that, the legal basis for the Data

national legislator would not allow the use of data originally stored to combat organized crime and terrorism[27] to enforce private intellectual property rights in the end.

While this can be seen as an important victory for privacy, it also has its downsides: Such a legislation renders the IP Enforcement Directive entirely ineffective in Internet cases. Arguably, no "balance" is struck at all here. Right holders have already approached the European Commission with the issue of ensuring that the public interest in an adequate level of data protection "is properly reconciled with other important public policy objectives such as the need to combat illegal activities and to protect the rights and freedoms of third parties".[28]

At the same time, the "no, no, never" legislation adversely affects the legal awareness of Internet users. Because their identity is difficult to learn, they will, in a lot of instances, not get involved in individual litigation. They might not have and never get the awareness of acting illegally. Their sense for right and wrong continues to impair.

Retention Directive itself is contested before the E.C.J, see pending Case No. C-301/06.

[26] See the organized protest against data retention at http://www.vorratsdatenspeicherung.de.

[27] See *supra*, I A.

[28] See Communication from the Commission on Creative Content in Online the Single Market, COM(2007)836 final at 7.

III. Can the "Provider Does It All" Approach Strike the Right Balance?

Because IP enforcement against individual infringers becomes difficult if their identity is virtually impossible to obtain, the debate has now focused on installing filtering and blocking obligations for access providers.[29] The European Commission sympathizes with such obligations.[30] In France, filtering mechanisms are part of the so called Olivennes Memorandum of Understanding.[31] In Sweden, a government report recommends to oblige access providers to block the access of certain file sharers upon the request of right holders.[32] Similar discussions are currently taking place in other countries, e.g., in Japan[33] and in the United Kingdom[34].

---

[29] See *IFPI Digital Music Report 2008* (Making ISP Responsibility a Reality in 2008), at http://www.ifpi.org/content/library/DMR2008.pdf.

[30] See Communication from the Commission on Creative Content in Online the Single Market, COM(2007)836 final at 7.

[31] In France, a Memorandum of Understanding between music and film producers, Internet service providers and the Government was signed on 23 November 2007. Under the agreement, France is to set up a new Internet authority with powers to suspend or cut access to the web for those who illegally file-share, and access providers are to implement filtering and blocking instruments, see "Accord pour le développement et la protection des oeuvres et programmes culturels sur les nouveaux réseaux" – http://www.culture.gouv.fr/culture/actualites/index-olivennes231107.htm.

[32] See http://www.regeringen.se/sb/d/8588/a/86944.

[33] See http://www.yomiuri.co.jp/dy/national/20080315TDY01305.htm.

However, this solution also seems inadequate if one looks at the original conflict and at the parties involved in it: The original conflict lies between the person who infringes and the person whose rights are infringed, i.e.: between the individual user and the right holder. Under the "provider does it all" approach, the right holder has to argue with the access provider about the extent and implementation of filtering and blocking instruments. The access provider, on the other hand, has to argue with its client whose content is monitored and, if necessary, filtered or blocked. This solution makes two conflicts out of one, and it shifts these conflicts from the parties originally involved to a third party that is only remotely involved: to the access provider.

In addition, filtering solutions always imply some kind of monitoring of data traffic. This, again, brings up privacy issues. In Germany, e.g., the "secrecy of telecommunication" is a strongly protected constitutional right[35] the violation of which constitutes a criminal offense.[36]

Last, but not least, this solution may arguably pose an undue burden upon the access providers: They are not involved in the original conflict between right holder and infringer, and filtering and blocking illegal content is a complex exercise given the huge amount of traffic providers have to handle

---

[34] See http://www.ft.com/cms/s/0/26765228-e0c0-11dc-b0d7-0000779fd2ac.html?nclick_check=1.

[35] See Art. 10 (1) GG (Grundgesetz, Federal Constitution).

[36] See § 206 StGB (German Penal Code).

every day. For these reasons, Art. 15 (1) of the E-Commerce-Directive[37] clearly prohibits general monitoring obligations for service providers.[38]

IV. Proposal for a Two-Tiered System

In my view, a two-tiered system could strike a better balance. A two-tiered system would distinguish between first-time infringers and infringers who act repeatedly. The access provider would not be obliged to monitor data traffic generally, but would, upon the request of a right holder providing the IP address of an infringer, have to determine internally if the user is a first-time infringer or if the user has infringed repeatedly. Depending on the result, the further actions would be as follows:

The first stage would be applied to first-time infringers: In this case, the access provider would not be allowed to use the IP address to disclose the identity of the infringing user to the right holder or to any other external

[37] 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, 2000 O.J. (L 178) 1.

[38] Art. 15 (1) of the Directive reads: "No general obligation to monitor – Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity."

entity, be it private or governmental.[39] The access provider would, however, be obliged to send a warning notice to the infringing user. Because user data would stay with the access provider and not be disclosed externally, this would maintain a high level of privacy at first.

At the same time, it would raise the legal awareness of the user: The user learns that her actions have been noticed and that a right holder sees his copyright infringed by these actions.[40] The user will be informed that in the case of repeated copyright infringement her identity will be disclosed to the right holder which may result in civil proceedings. Since most infringers, once caught, never infringe again, the right holder will also profit from this warning message.

If the access provider finds in his records that the user does infringe repeatedly, stage two would commence. Instead of obliging the access

---

[39] This makes it different from the new Internet authority discussed in France, see "Accord pour le développement et la protection des oeuvres et programmes culturels sur les nouveaux réseaux" – http://www.culture.gouv.fr/culture/actualites/index-olivennes231107.htm.

[40] Because such a warning notice would come on an individual basis, it would be more effective than the general notice provided in Art. 20 (6) of the legislative proposal to amend the Universal Service Directive (COM(2007) 698 final). Art. 20 (6) proposes a general obligation for access providers to inform subscribers in advance of the conclusion of the contract and regularly thereafter of their obligations to respect copyright and related rights.

provider to block the user, the conflict should now be brought between the two parties who are really involved in it and who should settle it: between the right holder and the individual user. In stage two, the provider would have to – and, under privacy law: would be allowed to – disclose the identity of the user to the right holder. Even a traditionally strong privacy law cannot prevail over IP enforcement if the user has been warned and has intentionally continued to infringe copyright.

Such a two-tiered system would maintain a high level of privacy without making IP enforcement ineffective, it would raise the legal awareness of users without burdening access providers unduly. It would finally be in line with the proposal of the European Commission to instigate co-operation procedures between access providers and right holders[41].

[41] See Communication from the Commission on Creative Content in Online the Single Market, COM(2007)836 final at 8.