TILBURG UNIVERSITY

Obtaining information about copyright infringers from ISPs while safeguarding the privacy of internet users

What can Germany and the Netherlands learn from each other?

MASTER THESIS

S.J.A. Schroers

ANR 968149

Master Law&Technology

Master International Business Law

Thesis Supervisors: M.H.M. Schellekens, E.P.M. Vermeulen, J. Li

July 2012

Abstract

This thesis compares the procedures for obtaining information about copyright infringers from Internet Service Providers in Germany and the Netherlands. The differences in law and case law are discussed in the view of safeguarding the right of privacy of internet users. A small survey on the amount of requests for information in Germany and the Netherlands has been done and the possible reasons for the different outcomes between the two countries are explained. Further an overview of the introduction of IPv6 and how this could influence the procedures for obtaining information is given.

Preface

The topic of this thesis resulted from a during my study steadily growing interest in intellectual property law. I am fascinated by its implications on society and how on the other hand technology can influence law, like the implementation of IPv6. Furthermore I found during the research for this thesis that in the Netherlands it is up till today often assumed that in Germany the criminal procedure is the main way to enforce copyright, which is already since 2008 not the case anymore. So I hope this thesis can provide the reader some information of the different systems in Germany and the Netherlands for obtaining information about copyright infringers.

I thank my family and friends for their support.

Limitations of this paper:

Since the topic is more controversial in Germany than in the Netherlands, I could find more literature on it for Germany than for the Netherlands. For example could I find no actual information on the retention time of dynamic IP addresses in the Netherlands. Furthermore I found out during my research that in the Netherlands it is more common than in Germany to have static IP addresses as an end user, but I could find no information on how big this percentage is. Therefore I assume in this thesis that end users have for the most part dynamical IP addresses.

In this paper usually is the German or respectively Dutch way of writing articles of laws used, for the reason that this avoids translation mistakes and since most laws are not officially translated to English, it makes it easier to find them. An explanation of the German and Dutch words used is provided in Annex A.

Table of Contents

List of Abbreviations:

AG	Amtsgericht
Aw	Auteurswet
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BVerfG	Bundesverfassungsgericht
BW	Burgerlijk Wetboek
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EU	European Union
EC	European Commission
ECJ	European Court of Justice
FTP	File Transfer Protocol
GG	Grundgesetz
GKG	Gerichtskostengesetz
ID	Identifier
IANA	Internet Assigned Numbers Authority
ISP	Internet Service Provider
IP address	Internet Protocol address
IPv6, IPv4	Internet Protocol version 6, version 4
IETF	Internet Engineering Task Force
KG	Kammergericht Berlin (name of OLG Berlin)
LG	Landesgericht

LIR	Local Internet Registry
MAC	Media Access Control
NGO	Non-governmental organization
NIR	National Internet Registry
NTD	Notice and Takedown
OLG	Oberlandesgericht
OSI	Open Systems Interconnection
P2P	Peer to Peer
Rb	Rechtbank
RFC	Request for comments
RIR	Regional Internet Registry
StPO	Strafprozeßordnung
TCP	Transmission Control Protocol
TDDSG	Teledienstedatenschutzgesetz
TKG	Telekommunikationsgesetz
UrhG	Gesetz über Urheberrecht und verwandte Schutzrechte
Wbp	Wet bescherming persoonsgegevens

Introduction:

A copyright holder who finds out that somebody is up- or downloading his copyrighted work on the internet wants to stop this and maybe sue the copyright infringer. But the problem may arise that the only information about the infringer is his IP-address. Internet users are not recognizable by name, but by a number, the IP-address. Some internet users have a static IP-address, but most users get an IP-address 'dynamically' allocated per session. In that case only the ISP has the information about the person behind an IP-address at a specific date and time. To obtain the information that is needed to enforce his rights, the copyright holder will have to get this information from the ISP.

On the other hand, an internet user doesn't want that just anybody can obtain his personal information from the ISP. It would not be beneficial for privacy, nor for free speech, if anybody who for example does not like a comment of someone on internet, could inquire by the ISP personal information of that person.

A weighting needs to be made of which infringements of property right justify what kind of breaches of the right on privacy.

In this paper I will compare Germany and the Netherlands since they have different procedures upon this question. In Germany the copyright holder always needs to go to court to obtain the information from the ISP, while in the Netherlands it is under certain conditions possible for a right holder to obtain the information directly from the ISP.

The central question is, what can Germany and the Netherlands learn from each other regarding the problem of safeguarding privacy of internet users while giving copyright holders the information held by ISPs to identify perpetrators of copyright infringement?

To answer this question the paper will be divided in five chapters.

The first chapter gives explain the (technical) background related with this problem. This chapter will be based on desk study, using scholarly literature, articles, online sources, technical reports and interviews with experts.

In the second chapter, the different laws of Germany and the Netherlands as well as their case law will be presented. First the most important European Union Directives and two cases will be described. After that the development of the German system as well as its case law will be outlined. The same will be done with the Dutch system. At the end of this chapter, the differences in the decisions of the judges will be compared to find out where the judges in the Netherlands and in Germany set the fair balance between the rights of copyright enforcement

and privacy. This chapter will be based on desk study, using legislation, case law, policy papers and scholarly literature as sources.

The third chapter will show the actual situation in Germany and the Netherlands while trying to explain the findings of a survey. In order to get insight in the amount of requests for information towards the providers, several access provider in the Netherlands, XS4ALL, KPN, UPC, T-mobile and Ziggo[1], as well as the Stichting BREIN are asked for information. In Germany this is done with the four biggest access providers Telekom, 1&1, Vodafone and O2/Alice[2] and the courts located at the place of their head office, which according to § 105 UrhG in combination with the "Rechtsverordnungen der Bundesländer" and the decision of the OLG Düsseldorf[3], are usually the responsible courts for § 101 Abs. 9 UrhG requests. These are the LG Köln (Telekom Seat Köln), the LG Frankenthal (1&1 Seat Montabaur), the LG Düsseldorf (Vodafone Seat: Düsseldorf) and the LG München (o2/Alice: Telefonica Seat: München), and the ISP association eco e.V.. The outcome of the survey will be described and set into context with information about the Dutch and German society and their particular ways of enforcing copyright to conclude which system factually protects privacy better. This chapter will be based on the results of the survey and desk study, using scholarly literature, policy papers, but also non-scholarly literature like newspaper articles.

The fourth chapter will discuss IPv6. IPv6 is the new Internet Protocol (the follow up of IPv4) and has enough IP addresses to give a static IP address to every internet accessible device. This could theoretically make it easier for copyright holders to get hold of the internet user information. In this chapter the introduction of IPv6 and its' possible implications on the Dutch and German system will be described. This chapter is going to be based on policy papers, scholarly literature, articles and available expert and technical reports which information will be used to outline the background of IPv6 and its implications within the context of this paper.

In the fifth chapter the findings of the previous chapters will be discussed and a conclusion will be drawn upon this findings.

---

[1] XS4ALL (KPN):40%; UPC:14% and Ziggo: 26% : Marktverhoudingen breedbandtoegang Q3 2011. <http://nlkabel.nl/nl/Home/Cijfers-en-feiten/Internet.aspx>.

[2] Telekom: 45,4%; 1&1: 11,9%; Vodafone: 12,8%; O2/Alice:9,7% : Marktanteile der führenden Breitband-Anbieter in Deutschland Q3 2011 <http://www.dslweb.de/dsl-marktuebersicht.php>.

[3] OLG Düsseldorf, 8.12.2008 - Az. I-20 W 130/08.

Chapter 1: Background information

1.1. The Internet Protocol:

The Internet started with ARPANET, a decentral network which was realized in 1969 by the Advanced Research Projects Agency. It was based on a study upon a request of the United States Air force to determine how the Air Force could maintain command and control over its missiles and bombers in the event of a nuclear war. [4] The Internet started with the principal idea of messages being divided into separate building blocks, then sent to a remote area and then reassembled at a remote location. In 1973 the Transport Control Protocol (TCP)/Internet Protocol (IP) were developed. [5] The function of the TCP is to keep track of the individual "data packets", regulating the flow of the packets, error detection, retransmission and duplicate detection.[6] The Internet Protocols (IP) function is that of a communication protocol responsible for transporting data from its origin to its destination across the Internet.

OSI model:

7. **Application layer**: NNTP, DNS, FTP, HTTP etc.
6. **Presentation layer**: MIME, XDR, TLS, SSL
5. **Session Layer**: NetBIOS, SAP, PPTP etc.
4. **Transport layer**: TCP, UDP, SCTP, DCCP etc.
3. **Network layer**: IP (IPv4, IPv6), ARP, ICMP, IPsec etc.
2. **Data link layer**: ATM, SDLC, IEEE 802.2, IEEE 802.3, etc.
1. **Physical layer**: Basic networking hardware transmission technologies

[4] Foster Henderson: "*Understanding the Ramifications of IPv6" Ch.7 in edit. H. F. Tipton & M. Krause Nozaki "Information Security Management Handbook*", 6th edition, , volume 5, 2012 CRC Press, Boca Raton, p. 117.

[5] Foster Henderson: "*Understanding the Ramifications of IPv6" Ch.7 in edit. H. F. Tipton & M. Krause Nozaki "Information Security Management Handbook*", 6th edition, , volume 5, 2012 CRC Press, Boca Raton, p. 117.

[6] RFC 675, p.3.

The Open System Interconnection (OSI) reference model has seven layers.[7] The IP is on the third layer, the network layer. Unlike the TCP, the IP is a connectionless protocol. [8] To specify the locations of the source and destination nodes and to route messages the protocol uses a numeric addressing system, the IP addresses. Right now there are two versions of IP addresses in active use, IP version 4 (IPv4) and IP version 6 (IPv6). [9]

1.1.1. Allocation of addresses:

IP addresses are generally assigned in a hierarchical manner. On top stands the Internet Assigned Numbers Authority (IANA), which is responsible for the global coordination of the Internet Protocol addressing systems. The IANA delegates blocks of IP addresses from the pools of unallocated addresses to the Regional Internet Registry (RIR). This is done according to the needs of the RIRs as described by global policy and to document protocol assignments made by the Internet Engineering Task Force[10] (IETF)[11]. The regional communities establish and authorize internet registries, which then are recognized by the IANA to serve and represent these geographical regions. [12] The RIRs are the AfriNIC for the Africa Region, the APNIC for Asia/Pacific Region, the ARIN for the North America Region, the LACNIC for Latin America and some Caribbean Islands and the RIPE NCC for Europe, the Middle East and Central Asia[13]. The RIRs then allocate resources, following regional policies, to the third layer, the Local Internet Registries (LIRs) or in some countries to National Internet Registries (NIRs). Finally the LIRs either assign addresses to end users or allocate addresses to ISPs, who then assign IP addresses to enterprises and end users.[14]

---

[7] Foster Henderson: "*Understanding the Ramifications of IPv6" Ch.7 in edit. H. F. Tipton & M. Krause Nozaki "Information Security Management Handbook*", 6th edition, , volume 5, 2012 CRC Press, Boca Raton, p. 118.

[8] Foster Henderson: "*Understanding the Ramifications of IPv6" Ch.7 in edit. H. F. Tipton & M. Krause Nozaki "Information Security Management Handbook*", 6th edition, , volume 5, 2012 CRC Press, Boca Raton, p.119.

[9] OECD, "*OECD Communications Outlook 2011"*, 2011, OECD Publishing, p. 181.

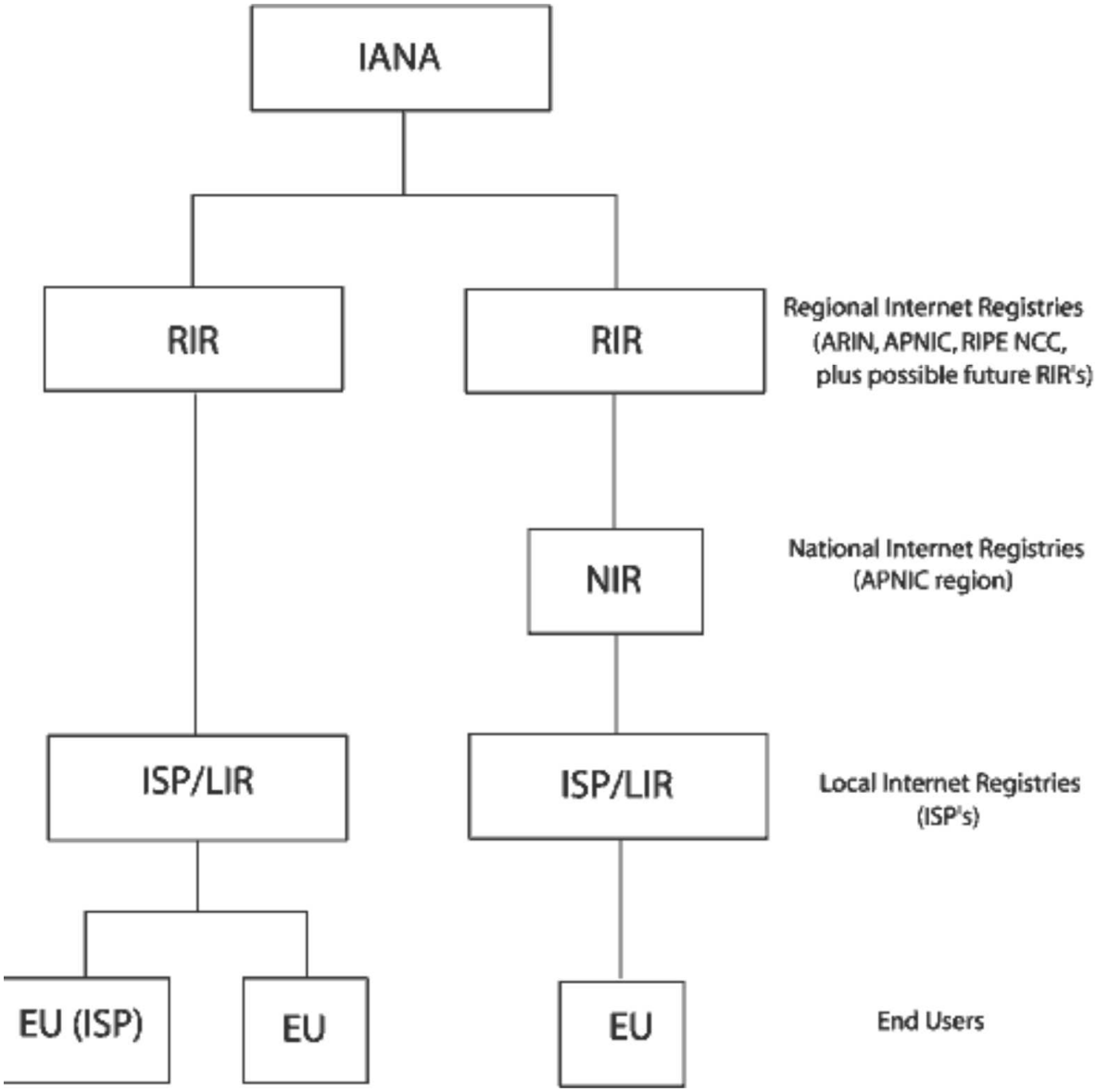
[10] "Internet Engineering Task Force (IETF) is an open global community of network designers, operators, vendors, and researchers producing technical specifications for the evolution of the Internet architecture and the smooth operation of the Internet", RFC 3233.

[11] Internet assigned number authority, <www.iana.org>.

[12] RIPE, "IPv6 Address Allocation and Assignment Policy"; RIPE 552, May 2012, p.3.

[13] Internet assigned number authority, <www.iana.org>.

[14] OECD, "*OECD Communications Outlook 2011"*, 2011, OECD Publishing, p. 182.



Source: "IPv6 Address Allocation and Assignment Policy"; RIPE 552, May 2012, p.3.

WHOIS:

WHOIS is a protocol to look up data within a registries database. It was first described in 1982 in RFC 812 and the idea was to provide a central directory service to ARPANET users.[15] Since it was

[15] RFC 812, p.1.

in the beginning only intended for a trusted circle, it has no provisions for strong security.[16] The name of the protocol is often also used for the database queries. Nowadays different registries manage different databases[17]. The (blocks of) IP addresses are normally registered in the databases of the five RIRs and can be looked up with a WHOIS query[18].

1.1.2. IPv4:

IPv4 is an Internet Protocol which started to be deployed in 1983. It uses 32-bit addresses, generally expressed in decimal notation with each octet (group of eight bits) separated by a period (e.g. 137.56.157.10). Its address space is limited to 2^32 (4294 967 296) possible unique addresses.

At the time of deployment this amount seemed to be enough, but the unexpected big growth of the Internet led to an exhaustion of IP addresses. On 3 February 2011 the IANA distributed its last five IPv4 blocks to the five RIRs.[19]

The shortage of IPv4 addresses gave rise to creating several network techniques and technologies whose goal among others is to delay the exhaustion of the IPv4 pool[20]. For the scope of this paper probably the most important is the dynamic IP address allocation by the Dynamic Host Configuration Protocol (DHCP)).

DHCP provides configuration parameters to Internet hosts.[21] It supports three mechanisms for IP address allocation, "automatic allocation", "dynamic allocation" and "manual allocation"[22]. Dynamic allocation allows automatic reuse of an address that is no longer needed by the client to which it was assigned, which is especially useful for assigning addresses to clients which are only temporarily connected to the internet or to share a limited pool of IP addresses among a

---

[16] RFC 3912, p. 2.

[17] For example registries for top level domains (like eurid manages .eu; denic manages .de; etc.).

[18] For example for RIPE: RIPE Network Coordination Centre, "RIPE Database Query", <https://apps.db.ripe.net/search/query.html>.

[19] RIPE Network Coordination Centre, "RIPE Database Query", <https://apps.db.ripe.net/search/query.html>.

[20] OECD, "*OECD Communications Outlook 2011"*, 2011, OECD Publishing, p. 182

[21] RFC 2131, p. 2.

[22] "Automatic allocation" means DHCP assigns a permanent IP address to a client, in "manual allocation" a client's IP address is assigned by the network administrator and DHCP is used to convey the assigned address to the client. (RFC 2131 p.3.).

group of clients that do not need permanent IP addresses.[23] For companies using permanent connections even with the usage of dynamic addresses in practice servers often return the same address to the same client.[24] For home users the situation is different, since they don't have permanent connections and get assigned different addresses each time they connect to their ISP. Therefore in that case an IP address does not reliably identify a particular device over time spans of more than a few minutes.[25] While static IP addresses are usually registered in databases, often with the registrants name and contact details and this information can mostly be looked up with WHOIS queries, the private internet user using dynamic IP addresses has the effect of relative anonymity, since he can't be identified directly via his IP-address.[26]

But even these techniques and technologies can not stop the exhaustion of IPv4 addresses, which is why the only long-term solution is the transfer to IPv6. IPv6 will be explained further in Chapter 4.

1.2. Definition Internet Service Provider

In principle is everybody who provides a service on the internet an Internet service provider.

In the literature are different types of Internet service providers described:

The *Network provider*, also known as internet backbone provider, is the provider who exploits the physical network/infrastructure.[27] The *Access provider* provides access to the internet for example by supplying his customers an IP-address and the possibility of data traffic via the TCP/IP protocol.[28] The *Service provider* provides technical possibilities like e-mail, news groups and webservers.[29] And an *Information* or *content provider* is everyone who provides

---

[23] RFC 2131, p.3.

[24] RFC 4941, p. 6.

[25] RFC 4941, p. 6.

[26] T. Hoeren, "*Anonymität im Web – Grundfragen und aktuelle Entwicklungen*", ZRP 2010, p. 253.

[27] L.A.R. Siemerink, "*De overeenkomst van Internet Service Providers met consumenten*", diss. Leiden: Kluwer 2007, p. 12.

[28] L.A.R. Siemerink, "*De overeenkomst van Internet Service Providers met consumenten*", diss. Leiden: Kluwer 2007, p. 13.

[29] L.A.R. Siemerink, "*De overeenkomst van Internet Service Providers met consumenten*", diss. Leiden: Kluwer 2007, p.13.

information on the internet.[30] Therefore everybody who uploads illegal content on the internet is in fact also an information provider.

On the other hand the E-commerce Directive distinguishes three types of services that providers can provide on the internet:

"Mere conduit": This type of service includes the transmission of information on - or the provision of access to a communication network.[31] These are for example the services an Access provider provides.

"Caching": This is a service which is used to make the internet faster. Caching means the "automatic, intermediate and temporary storage" of information.[32] The intermediary caches often requested information in the cache memory of his server in order to provide it faster.[33]

"Hosting": Means the storage of information provided by a recipient of the service.[34]

Art. 15 of the E-commerce Directive states that ISPs who provide these three types of services neither have a general obligation to monitor the information they transmit or store nor have to actively scan for indications of illegal activity.

Due to the hierarchical structure and the registration of the assignment of blocks of IP addresses to Internet Registries, it is possible to tell by the IP address to which region it was assigned and which ISP got it in his pool. That gives copyright holders the possibility to know which ISP they have to ask for the user information. Due to the dynamic allocation of IP addresses it is not possible to determine the identity or exact location of the user. With static IP addresses this is in principle possible, if the copyright holder has access to registries or databases where the address is saved.

---

[30] L.A.R. Siemerink, "*De overeenkomst van Internet Service Providers met consumenten*", diss.

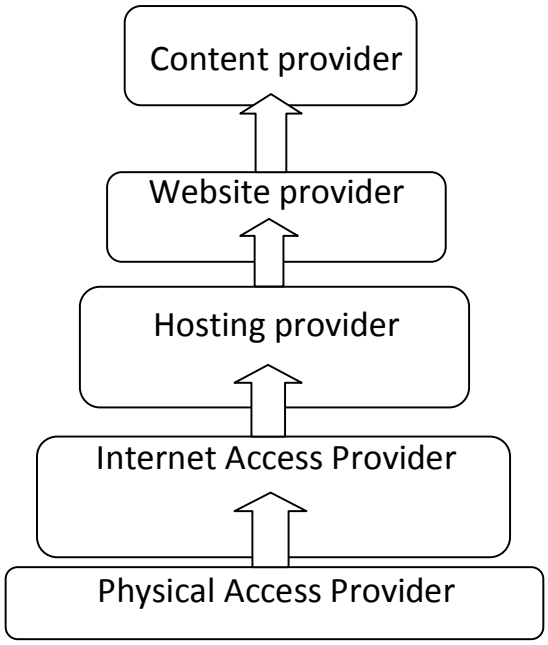
Leiden: Kluwer 2007, p. 14.

[31] 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, art. 12.

[32] 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, art. 13.

[33] L.A.R. Siemerink, "*De overeenkomst van Internet Service Providers met consumenten*", diss. Leiden: Kluwer 2007, p. 17.

[34] 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, art. 14.



Notice and Takedown Code of Conduct, version 1.04, 9 October 2008, p. 7.

To gain knowledge about a copyright infringer if only an IP address is known often the access provider will be approached since he has the information about which IP address was assigned to which customer at which time. An additional plus factor the fact that an access provider provides paid services so the customer information is usually correct. For free services customers often register with information which is unusable for enforcement purposes.

1.3. File sharing:

There are different kinds of copyrightable works, like writings, photography, sculptures, architecture, motion pictures, musical works, sound recordings, audiovisual works and computer programs. The type of works which rights are often infringed on internet and whose right holders try to prosecute the infringements are sound recordings (music), audiovisual works (movies), literary works and games.

The problem for these copyright holders is that their works can easily be shared on the internet. While still in the 80s illegal copies of works where usually only possible in the form of analog copies, this changed with the development of digitalization. The Fraunhofer-Institute developed

for example the mpeg format which allowed the compression of audio data (mp3)[35]. Sharing works became easier due the growing digitalization and the possibility to compress the data volume while at the same time having internet connections became more common for normal households and the speed of the connection increased. The prevalent way of infringing copyright on the internet nowadays is the usage of file-sharing. File sharing means the public or private sharing of computer data on a network.

Some of the most important services of the internet are the World Wide Web, E-mail, Data management and discussion forums. All these can be used for file sharing.

The seventh layer of the OSI model is the application layer, which includes different protocols like HTTP (Hypertext Transfer Protocol, for the World Wide Web), NNTP (Network News Transfer Protocol, used for Usenet, a discussion forum network) and FTP (File Transfer Protocol).

FTP is probably next to the Usenet one of the first used ways to share files. FTP is a simple client-server protocol, used to transfer data in TCP/IP based networks. The objectives of it were described in 1985 in RFC 959 as firstly to promote sharing of files (computer programs and/or data), secondly to encourage indirect or implicit (via programs) use of remote computers, thirdly to shield a user from variations in file storage systems among hosts, and lastly to transfer data reliably and efficiently.[36] The user connects with this protocol to another computer (server) inside a network (usually the internet).[37] After the user has been authenticated by the server he can within the boundaries of his access rights give commands to it. Every user can then upload data on the server and view and download data stored on it.[38] Requirement for viewing is an FTP-Client, which is integrated in most Browsers, for uploading programs like FileZilla are used. To find copyright protected material stored on the server, links are provided for example in Chat-Forums.[39]

---

[35] More information about it can be found on: Fraunhofer IIS, „The mp3 History", <http://www.mp3-history.com/>.

[36] RFC 959.

[37] G.R. Wick, *„Inhalt und Grenzen des Auskunftsanspruchs gegen Zugangsanbieter – Eine Untersuchung des § 101 UrhG unter besonderer Berücksichtigung der Filesharing-Systeme*", TGRAMEDIA, Bonn 2010, p. 17.

[38] G.R. Wick, *„Inhalt und Grenzen des Auskunftsanspruchs gegen Zugangsanbieter – Eine Untersuchung des § 101 UrhG unter besonderer Berücksichtigung der Filesharing-Systeme*", TGRAMEDIA, Bonn 2010, p. 17.

[39] A. Kramer, *„Zivilrechtlicher Auskunftsanspruch gegenüber Access Providern – Verpflichtung zur Herausgabe der Nutzerdaten von Urheberrechtsverletzern unter Berücksichtigung der Enforcement-Richtlinie*", Verlag Dr. Kovac, Hamburg, 2007, p. 10.

Usenet (Unix User Network) is a 1979 launched worldwide distributed Internet discussion system. The Usenet is the oldest network for sharing news and files. It was developed parallel to the predecessor of the internet and long before the World Wide Web. When the internet was released for civil use, the Usenet was converted to the TCP/IP of the internet. The Usenet works with decentral connected News servers, which altogether form the Usenet. The articles that users post to Usenet are organized into topical categories called newsgroups, which are logically organized into hierarchies of subjects. Every article which is uploaded via a news server gets redistributed from there via the network to the other news servers, which keep the article if they have the newsgroup. The alt.* hierarchy is a major class of newsgroups, containing all newsgroups whose name begins with "alt." (standing for "alternative", not confined to any specific subject or type in opposition to the big eight hierarchies: comp, misc, news, rec, soc, sci, humanities and talk[40]). Especially here can Binary newsgroups be found (alt.binaries). These are under-hierarchies with binary files. Binary files can contain any type of file, like e.g. images, sounds or compressed versions of other files.[41] The binary newsgroups are a relatively young development within the Usenet and are responsible for a big amount of traffic.[42]

The most commonly known method for file sharing is the **peer-to-peer (P2P) network**. In fact file-sharing and P2P networks are often used in everyday speech without much distinction, even though file-sharing also includes other ways than the usage of P2P networks.
On P2P systems content is typically exchanged directly over the IP network. There are centralized and decentralized P2P networks. Centralized networks work with server support, which is used for indexing functions. Computers administrate the search inquiries and if a user searches for a file, he will be directed to a peer while on the server the IP-address of the user will be saved. These networks are called centralized networks, because of their lack of ability to work without their central servers. A pure, dezentralized P2P network does not have clients or servers but only equal peer nodes that simultaneously function both as clients and as servers to the other nodes on the network. Hybrid P2P networks allow preferred nodes (supernodes).

The first prominent P2P system Napster was an example of the centralized model , after it other networks arised which where usually decentralized or hybrid. The at the moment most known networks are for example the eDonkey network (centralized) with the clients eDonkey and eMule, the Gnutella network (dezentralized) with the client LimeWire and the a bit younger

[40] Comp: computer science subjects; misc: miscellaneous groups; news: news topics; rec: recreational subjects; soc: sociological subjects; sci: science topics; humanities: humanities subjects; talk: controversial topics.

[41] Wikipedia, "Binary file", <http://en.wikipedia.org/wiki/Binary_file>.

[42] Gulli, "Usenet", <http://www.gulli.com/internet/filesharing/grundlagen/usenet>.

BitTorrent protocol with the clients BitTorrent and µTorrent.[43] The BitTorrent protocol is based on Torrents, Torrent portals (indexing sites), Trackers and peers. Peers are the users of the network, who offer the files (seeders) and download them (leechers).[44] Different to a lot of other P2P protocols the downloader automatically uploads the files again. Torrents are small files which direct/refer to other files (almost like a link).[45] The .torrent files include the information necessary to start a download via the BitTorrent P2P protocol. To find torrents faster, websites (so called torrent portals/indexing sites) are used on whose servers users can upload the .torrents. Well-known portals are for example The Pirate Bay and Mininova. Often, but not necessarily these sites also manage the trackers. Trackers facilitate the traffic between the different peers on a network and makes sure that the user on basis of the .torrent file is directed to the different users which offer parts of the file.[46] These are all unencrypted types of P2P networks, but also encrypted P2P networks do exist. These are often referred to as "darknets" or "F2F (friend to friend) networks".[47] Darknets are P2P networks in which IP addresses are not publicly shared.[48] Connections are either made between trusted peers or at least a smaller group of users than normal P2P, using non-standard protocols and ports or onion routing. A well known network client is Freenet.

Another way of file sharing nowadays is the use of **Sharehoster** (also named One-Click Hoster, File Hoster or Cyberlocker). Sharehoster are companies which possess a big capacity of free storage space on which files can be uploaded and also downloaded. Different to P2P networks the files are centrally downloaded from the server of the sharehoster, which results in a higher download speed than in P2P networks. The highest download speed is reserved for people who

[43] Gulli, "P2P", <http://www.gulli.com/internet/filesharing/grundlagen/p2p>.

[44] B.W.Schermer, M.Wubben, "*Feiten om te delen – digitale contentdistributie in Nederland*", Considerati, May 2011, p. 41.

[45] B.W.Schermer, M.Wubben, "*Feiten om te delen – digitale contentdistributie in Nederland*", Considerati, May 2011, p. 41.

[46] B.W.Schermer, M.Wubben, "*Feiten om te delen – digitale contentdistributie in Nederland*", Considerati, May 2011, p. 41.

[47] Gulli, "P2P", <http://www.gulli.com/internet/filesharing/grundlagen/p2p>.

[48] Jessica Wood, "*The Darknet: A Digital Copyright Revolution"*, XVI Rich. J.L. & Tech. 14 (2010), p. 17.

pay for access.[49] In January 2012 Megaupload, one of the biggest sharehoster was closed and the operator got arrested.[50]

1.4. How get Copyright holders hold of the IP address of an infringer?

IP addresses of infringers are often found in the environment of P2P networks. In Germany specialized companies monitor P2P networks with special software and save the IP address of users which download copyright protected works and due to the system of P2P networks upload it at the same time. For evidence reasons these companies often download then parts of the protected work from that IP address and make screenshots from that process. To be certain that the file includes a copyrighted work the "Hash-value"[51] is used.[52]

Chapter 2:

2.1. European Union:

2.1.1.: Directives:

In the context of copyright enforcement, different directives of the European Union are important.

Regarding privacy is **Directive 95/46/EC** of 24 October 1995 on *the protection of individuals with regard to the processing of personal data and on the free movement of such data* important. This Directive states in article 7 that Member States shall provide that personal data may be processed for example only if the data subject has unambiguously given his consent or processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are

[49] Gulli, "oneclickhoster", <http://www.gulli.com/internet/filesharing/grundlagen/oneclickhoster>.

[50] FBI National Press Releases, "Justice Department Charges Leaders of Megaupload with Widespread Online Copyright Infringement", 19. January 2012, <http://www.fbi.gov/news/pressrel/press-releases/justice-department-charges-leaders-of-megaupload-with-widespread-online-copyright-infringement>.

[51] The Hash-value can be compared to an algorithmic "fingerprint" of data files with which can be confirmed that data files have the same content.

[52] Digiprotect, "FAQ – digiprotect", <http://www.digiprotect.org/html/faq.html>.

disclosed; or processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1). Article 8 provides that Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

For copyright holders on the other hand are **Directive 2000/31/EC** of 8 June 2000 on *certain legal aspects of information society services, in particular electronic commerce in the Internal Market* (Directive on electronic commerce) and **Directive 2001/29/EC** of 22 May 2001 on *the harmonization of certain aspects of copyright and related rights in the information society* interesting. Directive 2000/31/EC provides in Article 18 that Member States shall ensure that court actions available under national law concerning information society services' activities allow for the rapid adoption of measures, including interim measures, designed to terminate any alleged infringement and to prevent any further impairment of the interests involved. Directive 2001/29/EC states for example in art. 8 that Member States shall provide appropriate sanctions and remedies in respect of infringement of copyright. They shall take the measures necessary to ensure that right holders can bring an action and/or apply for an injunction and, where appropriate, for the seizure of infringing material and shall ensure that right holders are in position to apply for an injunction against intermediaries.

On the other hand states **Directive 2002/58/EC** of 12 July 2002 concerning *the processing of personal data and the protection of privacy in the electronic communications sector* in article 5 that Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorized to do so for example to safeguard national security (i.e. State security), defense, public security, and for the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the electronic communication system. In article 6 it says that Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication or some allowed purposes like subscriber billing and interconnection payments, marketing electronic communications services with consent of the subscriber etc.

This provision is amended by **Directive 2006/24/EC** of 15 March 2006 on *the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC* (Data Retention Directive) in order to force operators of public telephone services and Internet service providers to store data which is necessary to trace and identify the source of a communication. This data should be retained for a period of between six month and two years. They should "ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law". Due to the fact that the directive lacks clarity with regard to three main issues, it is not limited. It does not define what is meant by "serious crime" and leaves this task to each Member State's national law, it does not limit access to retained data to specifically designated law enforcement authorities, as it refers only to "competent national authorities" and it leaves it up to each Member State's national law as to when access to data is permitted, all of which are relevant to copyright enforcement, depending on where the line is drawn in each of the three cases.[53] Further the Directive is of importance to the copyright enforcement because if the retention time of information is longer than before, it would in principle be possible for copyright holders to obtain information which without the Data retention Directive already would have been erased.

At last **Directive 2004/48/EC** of 29 April 2004 on *the enforcement of intellectual property rights* (IPRED) provides that Member States should ensure that the infringer or the provider of the service used for infringing, give the information on the origin and distribution networks of the goods or services which infringe an intellectual property right.

2.1.2. Case Law:

An important case of the ECJ regarding the question how these directives have to be interpreted, whether the ISPs are considered to give the information away or keep the privacy of their customers is the case of Promusicae[54].

Promusicae is a Spanish non-profit organization of producers and publishers of musical and audiovisual recordings and Telefonica, a Spanish ISP. Promusicae applied to the Madrid Commercial Court No. 5 for preliminary measures against Telefonica, in order to retrieve identities and physical addresses of certain persons whose IP address and date and time of connection Promusicae knew. Promusicae wanted to get this information because according to them these persons were copyright infringers by engaging in peer-to-peer file-sharing and providing in shared files of personal computers access to phonograms in which the members of

[53] S. Larsson, "*The path dependence of European copyright*", Scripted Volume 8, Issue 1, April 2011, p. 22.

[54] Case C-275/06, Productores de Música de España (Promusicae) v Telefónica de España SAU.

Promusicae held the exploitation rights. For this reason, Promusicae wanted to bring civil proceedings against these persons. The Spanish court ordered the preliminary measures which were requested, but Telefonica appealed against that order on the ground that Spanish law authorized the communication of such data only in a criminal investigation or for the purpose of safeguarding public security and national defense, but not in civil proceedings.

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

Member States can therefore decide by themselves whether they shall provide in their national laws for an obligation for ISPs to communicate personal data to right holders (or those deriving their rights from them) in order to ensure effective protection of copyright in the context of civil proceedings or not, as long as they stay within the boundaries of the fundamental rights. In any event (and upon a weighting of the various rights involved), such an obligation is not dictated by European Union Law.[55]

This was further confirmed in the recent case of Bonnier Audio[56]. In this case the applicants were publishing companies holding the rights of audio books which were illegally distributed by an FTD server. The applicants tried to get the name and address of the person behind the IP address from which the infringing files were sent, but the service provider did not accept it and claimed that it would be against Directive 2006/24/EC. To the European Court the questions were referred "whether Directive 2006/24 is to be interpreted as precluding the application of a national provision based on Article 8 of [Directive 2004/48] which, in order to identify a particular subscriber, permits an internet service provider in civil proceedings to be ordered to give a copyright holder or its representative information on the subscriber to whom the internet service provider provided an IP address which was allegedly used in the infringement,

---

[55] I.A.Stamatoudi, "*Data Protection, Secrecy of Communications and Copyright*", in I. A. Stamatoudi (red.), "*Copyright Enforcement and the Internet*", Alphen aan de Rijn: Kluwer Law International 2010, p. 221.

[56] Case C-461/10, Bonnier Audio vs. Perfect Communication, 19 April 2012.

and whether the fact that the Member State concerned has not yet transposed Directive 2006/24, despite the period for doing so having expired, affects the answer to that question".[57]

The Advocate General stated in his opinion that his interpretation of the Promusicae case is that the basic principles of each domain – namely the protection of the confidentiality of electronic communication and the protection of copyright and related rights – must be observed in full.[58] For the disclosure of personal data to be possible, EU law requires that an obligation to retain data be provided for in national law, in order to specify the types of data to be retained, the purposes of retaining the data, the period of retention and the persons with access to said data. It would be contrary to the principles of the protection of personal data to make use of databases that exist for purposes other than those thus defined by the legislature.[59] He stated that national legislation must provide in advance and in detail restrictions to the scope of the rights and obligations in order for the retention and transmission of personal data and that this restriction must constitute a measure that is necessary, appropriate and proportionate. He emphasizes that the fundamental rights concerning the protection of personal data and privacy on the one hand and those concerning the protection of intellectual property on the other hand must receive equal protection, and concludes it with the opinion that copyright holders must not be favored, by allowing them to make use of personal data which have been legally collected or retained for other purposes than the protection of their rights. This kind of obligation would not be sufficient to meet the said requirements of the restriction and it is the responsibility of the national court to verify the existence of such measures and to ensure that they conform to those requirements.[60]

The court ruled that the application of national legislation permitting the order of ISPs in civil proceedings to identify an internet subscriber via his IP address which has been used in an infringement is not precluded by the application of Directive 2006/24/EC. It further states that "Directives 2002/58/EC and 2004/48/EC must be interpreted as not precluding national legislation such as at issue insofar as the legislation enables the national court seised of an application for an order for disclosure of personal data, made by a person who is entitled to act,

[57] Case C-461/10, Bonnier Audio vs. Perfect Communication, 19 April 2012, 36.

[58] Opinion of Advocate General Jääskinen, Case C-461/10, 17.11.2011, 59.

[59] Opinion of Advocate General Jääskinen, Case C-461/10, 17.11.2011, 60.

[60] Opinion of Advocate General Jääskinen, Case C-461/10, 17.11.2011, 61 &62.

to weigh the conflicting interests involved, on the basis of the facts of each case and taking due account of the requirements of the principle of proportionality".[61]

2.2. Law in Germany:

2.2.1. Private copy:

Copyright law is in Germany codified in the "Gesetz über Urheberrecht und verwandte Schutzrechte" (UrhG). In section 6, the limits of copyright like the private copy exemption are specified. The right on a private copy is regulated in Germany under § 53 UrhG ("Vervielfältigungen zum privaten und sonstigen eigenen Gebrauch", copying for private or other own use). It states in Abs. 1 that it is "allowed for a natural person to copy works for private use on any medium, provided it does not directly or indirectly serve commercial purposes and provided no apparent illegal produced or made publicly available original is used". The "apparent illegal produced" was added in 2003 and making a copy from an "apparent illegal made public available original" became forbidden in 2008 in order to discourage illegal file sharing.[62] In § 54 UrhG is provided that as compensation for the home copy exception an obligation to pay remuneration exists. These levies have to be paid by the producers of blank carriers or devices used for copying works.

2.2.2. File sharing:

In Germany uploading a copyrighted work without having the right is an infringement. It infringes the rights of the copyright owner, more specific the distribution right (§ 17 UrhG) and the right to make available to the public (§ 19a UrhG). If the uploader received the work illegally, for example by downloading it, then he also infringes § 96 UrhG (prohibition to exploit illegally made or obtained works) if he uploads it. This often happens in P2P networks, since downloaders upload at the same time. In case of file-sharing the uploader also infringes § 53 Abs. 6 UrhG if he received the work under the private copy exemption.

---

[61] Case C-461/10, Bonnier Audio vs. Perfect Communication, 19 April 2012, 61.

[62] *Zweites Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft*, 26.10.2007, BGBl I S. 2513, in force since 1.1.2008. Commonly nicknamed "Zweiter Korb"(second basket).

Downloading a copyrighted work is also illegal, if the source is "apparent illegal made public available" (§ 53 UrhG). "Apparent illegal made public available" is usually given in the environment of P2P file sharing, since it is for a normal person apparent that it is public available and not very likely that the uploader has the right to upload the work.[63] By downloading § 16 UrhG, the right of reproduction, will be infringed, which is criminal under §§ 106 ff. UrhG. Due to § 109 UrhG will such cases only be prosecuted upon request. Only in cases of public interest will the criminal prosecution authorities act on their own motion.

2.2.3. Information from an ISP based on an IP address:

Until 2008 a right holder in Germany had to start a criminal procedure (charge against a person unknown) to get information about the identity of the right infringer. The right holder could get the information by accessing the records, after the public prosecutor summoned the provider to give the identity information of the infringer, and start a civil procedure. This resulted in a high workload for the public prosecutors due to which more and more public prosecutors did not accept the claim for lack of suspicion ("mangelnder Tatverdacht") or denied access to the records based on § 406e Abs.2 StPO[64]. KG Berlin[65] ruled on the 25.9.2006 that name and address are customer data in the sense of § 5 Satz 1 Teledienstedatenschutzgesetz[66] (TDDSG), in which case due to § 5 Satz 2 TDDSG the information may only be given to law enforcement authorities and courts for the purpose of criminal enforcement. The court also decided that it is not possible to derive from § 242 BGB ("Leistung nach Treu und Glauben", good faith) nor from § 101a UrhG ("Anspruch auf Vorlage und Besichtigung", right of the right holder in case of copyright and similar infringements to have the infringer show him documents or give him access to places) analogue a claim to get information about the name or address of responsible persons for an internet page with manipulated pictures of a person.

---

[63] G.R. Wick, „*Inhalt und Grenzen des Auskunftsanspruchs gegen Zugangsanbieter – Eine Untersuchung des § 101 UrhG unter besonderer Berücksichtigung der Filesharing-Systeme*", TGRAMEDIA, Bonn 2010, p.26;

A. Ringnalda, M. Elferink & M. de Cock Buning, "*Auteursrechtinbreuk door P2P filesharing - Regelgeving in Duitsland, Frankrijk en Engeland nader onderzocht*", Centrum voor Intellectueel Eigendomsrecht, 10 July 2009, p. 71.

[64] § 406e Abs.2 StPO states that inspections of the records shall be refused if it would conflict with legitimate interests of the accused or other persons.

[65] KG Berlin, 25.9.2006 – Az. 10 U 262/05.

[66] The Teledienstedatenschutzgesetz was the German Tele Service Data Protection Act, but it got replaced in 2007 by the Telemediengesetz (Tele Media Act). § 14 Absatz 2 of the Telemediengesetz states now that the service provider may give information about customer data if it is necessary for criminal enforcement, [...] and for enforcement of intellectual property.

Since this way of enforcing copyright did not work satisfactory some amendments were introduced during the implementation of the directive 2004/48/EC. On 1st September 2008 the law to improve the enforcement of rights of intellectual property[67] came in to force which amended § 101 UrhG:

§ 101 Right to information[68]

(1) Whoever unlawfully infringes on a commercial scale copyright or other rights protected under this Act, may face a claim of the injured party of prompt disclosure of the origin and distribution of the infringing copies or other products. The commercial scale can arise both from the number of violations and the seriousness of the violation.

(2) In cases of obvious infringements or in cases where the injured party has brought action against the violator, the entitlement irrespective of paragraph 1 also against a person who on a commercial scale

1. had infringing copies in their possession,
2. was using infringing services,
3. **provided services used for infringing activities or**
4. was according to the statement of a in nr. 1, 2 or 3 named person involved in the production, manufacture or distribution of such copies, other products or services, unless the person would be under § § 383-385 of the Code of Civil Procedure be entitled to refuse to testify in a case against the violator. In the case of judicial enforcement of the claim pursuant the first sentence, the court may at request suspend the pending litigation against the offender until a final decision is reached in the litigation on the right to information. The party obliged to give information can claim from the injured party the necessary expenses for the provision of information.

[(3) …(8)]

(9) If the information can only be given under usage of traffic data (§ 3 No. 30 of the Telecommunications Act), is for granting it a prior court decision required which sees upon the admissibility of the use of traffic data, and needs to be requested by the injured party. For issuing this order is solely responsible the district court (Landgericht) in whose district the party required to give information resides, has his seat or an office, without regard to the sum in dispute. The decision is made by the civil division. For the procedure, the provisions of the "Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit" shall apply mutatis mutandis. The costs of the court order rest upon the requesting party. Against the decision of the District Court is appeal admissible. The appeal must be filed within a period of two weeks. The rules for the protection of personal data remain for the rest unaffected.
(10) By paragraph 2 in conjunction with paragraph 9, the basic right of telecommunications secrecy (Article 10 of the GG) shall be restricted.

---

[67] *Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums*, Drucksache 279/08, 02.05.2008, BGBl I, S. 1191, in force since 1.9.2008.

[68] own translation, bold parts added. For a complete translation of § 101 UrhG with the subparagraphs 3 till 8 see Annex B.

Right holders may now bring a claim under § 101 Abs. 2 UrhG to request disclosure of the identity of users.

For a claim based on § 101 Abs. 2 UrhG the requestor needs have the right to sue ("Aktivlegitimation"). This right has normally the copyright holder or an exclusive licensee. The capacity to be sued ("Passivlegitimation") have all parties named in the numbers 1 till 4 of § 101 Abs. 2 UrhG[69], therefore also ISPs. There need to be an infringement (usually in case of file sharing it is the infringement of § 19a UrhG), which needs to be illegal[70]. Further the requestor needs to either already have started a procedure against the infringer or the infringement needs to be obvious. Finally the infringement needs to be on a commercial scale in order to have a claim towards an ISP based on § 101 Abs. 2 UrhG[71].

As a safeguard for the secrecy of telecommunication § 101 Abs. 9 UrhG was implemented. It states that in case the disclosure of information is only possible with usage of traffic data (§ 3 nr 30 Telekommunikationsgesetz (TKG)) the civil court ("Landgericht") has to decide beforehand if the use of these traffic data is permissible ("Richtervorbehalt"). During the legislative procedure the Bundesrat objected to this "Richtervorbehalt" and stated it was alien to the system, burdens the courts and imposes considerable costs on the claimant. [72] Still the "Richtervorbehalt" was implemented and in the motivation of the draft legislation it has been justified with the fact that ISPs and telecommunication companies should be relieved of the decision whether an infringement is at hand or not.[73] Further it was motivated that traffic data has a special need of protection and is part of the constitutional safeguarded secret of

---

[69] G.R. Wick, „*Inhalt und Grenzen des Auskunftsanspruchs gegen Zugangsanbieter – Eine Untersuchung des § 101 UrhG unter besonderer Berücksichtigung der Filesharing-Systeme*", TGRAMEDIA, Bonn 2010, p. 37.

[70] Normally infringements implies the illegality, but there can exceptions arise due to reasons of justification (like e.g. ex post authorization).

[71] The Bundesrat was against the limitation to a commercial scale, but it stayed in the final law; Bundesrat, *Empfehlungen der Ausschüsse*, Drucksache 64/1/07, 26.02.2007, p. 19.

[72] Bundesrat, *Stellungnahme des Bundesrates*, Drucksache 64/07 (Beschluss), 9.3.2007, p.8.

[73] Bundesrat, *Gesetzentwurf der Bundesregierung*, Drucksache 64/07, 26.1.2007, S. 93.

telecommunication.[74] Due to this under these circumstances the disclosure of user data by an ISP without intervention of a judge would be a violation of telecommunication secrecy.[75]

2.2.4. Data retention:

On 1 January 2008 the law to implement Directive 2006/24/EC[76] on data retention came into force. By changing the federal code of Criminal Procedure, the law broadened the access authorization which regulated the access to retained data by non-intelligence law enforcement. In place of the "serious crimes" condition, law enforcement would have access to the data "if facts justify the suspicion that someone has committed a crime of considerable seriousness or a crime using telecommunications". This means that access to retained data could be justified for any crime involving telecommunications provided that investigating the issue or determination of the guilty party's location would otherwise be unpromising. [77] Within the Telecommunications law it introduced among other changes the § 113a TKG and § 113b TKG, which see upon the duty of telecommunication provider to retain and to communicate the retained data. Two month after the Bundestag approved the measure, the newly formed NGO 'Arbeitskreis Vorratsdatenspeicherung' (Working Group on Data Retention) filed a formal constitutional complaint at the Federal Constitutional Court in Karlsruhe with 34.000 complainants.[78] [79] On 11 March 2008 the Federal Constitutional Court issued a temporary injunction which allowed that communication data would be retained and saved by the providers, but prohibited the release to law enforcement bodies.[80] On 2 March 2010 the Federal Constitutional Court announced its decision. It nullified the law implementing the

---

[74] Bundesrat, *Gesetzentwurf der Bundesregierung*, Drucksache 64/07, 26.1.2007, S. 93.

[75] C. Kuner, C. Burton, J. Hladjk, O. Proust, "*Study on Online Copyright Enforcement and Data Protection in selected Member States", for DG Internal Market of the European Commission"*, November 2009, p. 34.

[76] *Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007*, BGBl I S. 3198, in force since 1.1.2008.

[77] C. De Simone, "*Pitting Karlsruhe against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive*", German Law Journal, Vol. 11 No. 3, p.305.

[78] As German procedural law does not recognize class-action lawsuits, these were considered as 34,000 separate suits.

[79] C. De Simone, "*Pitting Karlsruhe against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive*", German Law Journal, Vol. 11 No. 3, p. 306.

[80] BVerG, 11.3.2008 – Az. 1 BvR 256/08.

directive and ordered data retained under the interim ruling deleted.[81] On 7 June 2011 the Federal Ministry of Justice proposed a new law "Gesetz zur Sicherung vorhandener Verkehrsdaten und Gewährleistung von Bestandsdatenauskünften im Internet". Up until now no new law has been passed.[82]

2.2.4.1. Can information retained under the data retention law be accessed?

Information retained under § 113a TKG (duty for telecommunication providers to retain data, introduced by the data retention law) can not be used for the request of copyright holders in a civil law procedure. The Bundestag explicitly did not follow the suggestion of the Bundesrat to allow the use of the retained data also for copyright holders.[83] OLG Frankfurt am Main[84] ruled on 12 May 2009 that the § 101 Abs. 9 UrhG can only be used for the due to § 96 TKG[85] retained traffic data, not for the on the basis of § 113a TKG retained data. This was confirmed by the Federal Constitutional Court in its decision of 2 March 2010 which stated that the use of the under § 113a TKG retained data is excluded from the civil law information right of § 101 Abs. 9 UrhG.[86]

2.2.4.2. Normal length of data retention for copyright purposes?

§ 97 TKG declares that service providers can retain traffic data as long as the data is needed for the calculation of payment and for charging. In sentence 3 of § 97 TKG is stated that the service provider can retain the needed data up until 6 month after sending the bill (in case the customer raises objections the data can be retained until the objection is cleared). Data not needed for charging has to be deleted immediately.

In 2005 a customer of T-Online filed a lawsuit against T-Online because the company retained his data even though he had a flatrate for internet. The AG Darmstadt[87] decided that the

---

[81] BVerfG, 2.3.2010 – Az. 1 BvR 256/08.

[82] Beck-aktuell Gesetzgebung, „Entwicklungsgeschichte", <http://gesetzgebung.beck.de/node/1014619>.

[83] Deutscher Bundestag, *Beschlussempfehlung und Bericht*, BT-Dr 16/6979, 7.11.2007, p. 46.

[84] OLG Frankfurt am Main, 12.05.2009 - Az. 11 W 21/09, MMR 2009, 542.

[85] § 96 TKG states that Service Provider have to immediately delete traffic data if it is not further needed for the connection. Keeping data is allowed for technical and billing services, for marketing only if the customer allows it and it is anonymized.

[86] BVerfG, 2.3.2010 – Az. 1 BvR 256/08, Abs. 46.

[87] AG Darmstadt, 1.7.2005 – Az. 300 C 397/04.

retention of his data is illegal since it is not used for charging. In appeal the LG Darmstadt[88] confirmed this judgment and excluded appeal. T-Online tried with a complaint against denial of leave to appeal ("Nichtzulassungsbeschwerde") at the Federal Court of Justice to be admitted to appeal, but the Federal Court of Justice[89] refused the complaint and the decision of the LG Darmstadt became legally binding.

The Federal Court of Justice decided in his judgment of 13 January 2011[90] that retention limited to 7 days for technical or security reasons can be deemed proportional. Therefore it depends upon the decision of the ISP how long the traffic data will be retained, with a maximum of 7 days.[91]

2.2.5. Case Law:

2.2.5.1. The status of IP-addresses and the connecting identity information:

In Germany the question arose if IP-addresses and the connecting identity information are customer data or traffic data. § 3 nr. 3 TKG defines customer data ("*Bestandsdaten*") as data of a subscriber which is used for motivation, form, changes or termination of telecommunication services[92]. § 3 nr 30 TKG defines traffic data ("*Verkehrsdaten*") as data which by providing telecommunication services is compiled, processed or used[93]. This difference is of importance for the request of data, since depending on the type of data, different protection is given to it.

LG Offenburg[94] decided on 17 April 2008 in case of a request of the public prosecution department to get information about the person behind an IP address, that due to the new law to implement Directive 2006/24/EG it can be concluded that the data is customer data.

---

[88] LG Darmstadt, 25.1.2006 – Az. 25 S 118/2005.

[89] BGH, 26.10.2006 – Az. III ZR 40/06 vom 26. Oktober 2006.

[90] BGH, 13.1.2011 – Az. III ZR 146/10; MMR 5/2011.

[91] Deutsche Telekom: 7 days; Alice/O2: 7 days; 1&1: 7 days; Vodafone: does not retain (source: Netzwelt, "IP-Speicherfristen: Wie lange speichern die Anbieter?", <http://www.netzwelt.de/news/91086-ip-speicherfristen-lange-speichern-anbieter.html>).

[92] § 3 nr. 3 TKG *„Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden"*

[93] § 3 nr. 30 TKG *„Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden"*

[94] LG Offenburg, 17.04.2008 - Az. 3 Qs 83/07.

In May 2008 the LG Frankenthal[95] on the other hand decided that the IP-address is not customer data but traffic data in the sense of §§ 3 nr. 30, 96 Abs. 1 nr. 1 TKG because it is used in connection of usage of telecommunication services and therefore has a stricter protection (secrecy of telecommunications (("Fernmeldegeheimnis") Art. 10 GG). This data may only be given from the provider to law enforcement authorities and courts in case of suspicion of a severe criminal offense in the sense of § 100a Abs. 2 StPO. In case of copyright is it not applicable. The court interpreted the decision of the Federal constitutional court on the question of data retention[96] in a way that already the demand for these data would be a grave and irreparably interference of the basic right of Art. 10 Abs. 1 GG. But this decision got revoked by the OLG Zweibrücken[97] on 26. November 2008, which decided that the demand is not in interference with basic rights and that the copyright holder should have the possibility to get the information about who the user behind a certain IP address at a certain time was.

In July 2008 the LG Stralsund[98] decided again that IP-addresses are traffic data, which fall under the secrecy of telecommunications. But users of file sharing networks voluntarily give up their legally protected interest because during the use the data is given away freely and can be seen by everybody. The information about name or address is customer data, which doesn't fall under the secrecy of telecommunications.

In the draft legislation of the federal government considering the introduction of § 101 Abs. 9 UrhG it was specially stated that IP addresses are traffic data which are subject to the secrecy of telecommunication.[99] The Bundesrat on the other hand stated that the traffic data is already known by the claimant, the information asked is customer data, which is not protected by the secrecy of telecommunication.[100] The opinion that dynamic IP addresses are traffic data and names and addresses of customers are customer data is now mostly followed, especially since also the Federal Court of Justice and the Federal Constitutional Court acknowledged it.[101]

---

[95] LG Frankenthal, 21.5.2008 – Az. 6 O 156/08.

[96] BVerG, 11.3.2008 – Az. 1 BvR 256/08.

[97] OLG Zweibrücken, 26.9.2008 - Az. 4 W 62/08.

[98] LG Stralsund, 11.7.2008 – Az. 26 Qs 177/08.

[99] Bundesrat, *Gesetzentwurf der Bundesregierung*, Drucksache 64/07, 26.1.2007, S. 93.

[100] Bundesrat, *Stellungnahme des Bundesrates*, Drucksache 64/07 (Beschluss), 9.3.2007, p.9.

[101] BGH 13.1.2011 – Az. III ZR 146/10, MMR 5/2011; BVerfG, 02.03.2010,- Az. 1 BvR 256/08.

But the question whether the conjunction of the IP address at a certain time and the name and address of a customer is covered by the rules for customer data or by the rules for traffic data seems up until now still to be unanswered.[102] The usual reasoning is that even if the requestor has already obtained the IP address, to give the requested customer information the ISP needs to access the logfiles, which fall under the protection of the secrecy of telecommunication. That's why for this act the "Richtervorbehalt" is necessary.

Since for a static IP address the logfiles do not need to be accessed they are considered customer data and not traffic data. This opinion has been confirmed by LG München in May 2011.[103]

2.2.5.2. When is an infringement "obvious"?

The question of obviousness is important since due to § 101 Abs. 2 UrhG third parties can only be requested for information if the infringement is obvious.

The Federal government stated in its draft of legislation that an infringement is obvious if it is so unambiguous that an unjustified burden on third parties seems to be impossible. It states that in such a case the infringer about whom the third party has to provide information is not entitled to protection, especially since in case of doubts in factual or legal respects the obviousness of an infringement can never be assumed.[104]

The LG Hamburg decided on 11.3.2009[105] that the infringement is obvious, if considering the factual circumstances as well as the legal assessment the likeliness that a violation has already been established, is considered to be certain to such an extent that a wrong decision, and therefore an unjustified burden on the claim opponent, seems to be excluded.

In the perception of the LG Köln on 30.4.2009[106] this also means that an information can not be given if there are doubts on the existence of an infringement on a commercial scale.

---

[102] C. Czychowski, J. Nordemann; *Use of retained data and copyright law in Germany – the German data protection problem to fight internet piracy*; E.I.P.R. 2010, 32(4), 174-177.

[103] LG München, 24.05.2011 - Az.: 21 O 9065/11.

[104] Deutscher Bundestag, *Gesetzentwurf der Bundesregierung*, BT-Drs. 16/5048, 20.4.2007, p. 39.

[105] LG Hamburg, 11.03.2009 - Az. 308 O 75/09.

[106] LG Köln, 30.04.2009 - Az. 9 OH 388/09 .

That the infringement is obvious is in practice concluded from the fact that the applicant delivered an expert opinion and other documents which conclude that the detection software used is reliable, the software has been properly used in operation and has led to the finding of the IP addresses at the specific point in time and that there is no reason to doubt this findings.[107]

That the person behind the IP address at that point of time really did commit the infringement needs not to be proven. Only the obviousness of the infringement has to be proven.[108]

2.2.5.3. Commercial scale:

Most difficult is the question whether the infringement was on a commercial scale. This is requirement for a third party request based on § 101 Abs. 2 UrhG. § 101 Abs. 1 UrhG states that commercial scale can be defined both by the number of violations and the seriousness of it.

Neither of those criteria is further defined. LG Frankenthal decided on 15.9.2008[109] that commercial scale can not be assumed below an amount of 3000 music files or 200 movies. These numbers were based on a recommendation in criminal cases, but it has been criticized that this can not be used for civil cases.[110] So no exact definition of an amount of infringements exists.

On the question of the seriousness exists a lot of different case law. The Bundestag wrote in it's recommendation that an infringement can be considered serious if an considerably extensive data file like for example a complete cinema movie or music album or audio book before or directly after its release in Germany has been illegally made public on the internet.[111]

So already shortly after the amendment of § 101 UrhG decided the LG Köln on 2.9.2008[112] that a copyright infringement on a commercial scale in the sense of § 101 Abs. 1 UrhG[113], if a sound

---

[107] OLG Karlsruhe, 01.09.2009 - Az. 6 W 47/09; OLG Köln, 21.10.2008 - Az. 6 Wx 2/08; OLG Köln, 10.1.2012 – Az. 6 U 242/11.

[108] OLG Zweibrücken, 21.09.2009 - Az. 4 W 45/09.

[109] LG Frankenthal, 15.09.2008 - 6 Az. O 325/08.

[110] See: G.R. Wick, „*Inhalt und Grenzen des Auskunftsanspruchs gegen Zugangsanbieter – Eine Untersuchung des § 101 UrhG unter besonderer Berücksichtigung der Filesharing-Systeme*", TGRAMEDIA, Bonn 2010, p. 52.

[111] Deutscher Bundestag, *Beschlussempfehlung und Bericht des Rechtsausschusses (6. Ausschuss) zu dem Gesetzentwurf der Bundesregierung*, BT-Drucksache 16/8783, 09. 04. 2008, p. 50.

[112] LG Köln, 2.9.2008 - AZ. 28 AR 4/08 (aufgehoben).

storage medium has been made publicly available before or shortly after its official release in Germany.

A few days later the LG Köln decided on 5.9.2008[114] that already the publication of a single data file can be considered „commercial scale“ if it is still a particular highly demanded music album even though the music album has already been a year on the market.

The LG Bielefeld on 11.9.2008[115] determined it even stricter and decided that already the making available of a single data file on a file-sharing platform can be considered commercial scale. The LG Oldenburg[116] followed this opinion. The court decided that the making available on file-sharing platforms is always a commercial scale infringement, since for the acting person it is not important who can access the data files. The border to private actions has been surpassed as soon as the file is made available to an unclear and unlimited group of people.

On 17.12.2008 the LG Köln[117] decided that also in case uploading of the copyright protected work, has not been done shortly before or after the release of the work, it can be an infringement of a commercial scale if that work is still listed high in the selling charts and a further exploitation is planned.

On 9.2.2009 OLG Köln[118] stated that the making publicly available of a work which is already four years on the market can still from an infringement on commercial scale, if it is a timeless classical work which is still sold at a usual price.

Not so long ago the OLG München[119] decided on 26.7.2011 that an infringement which is done by offering a data file with copyright protected material on a file sharing platform, is generally an infringement on commercial scale, without the need of further aggravating circumstances.

Even though it seems as if the interpretation of “commercial scale” gets more broad, there are also some court decisions which restrict it.

---

[113] § 101 Abs. 2 UrhG serves the assertion of § 101 Abs. 2 UrhG, therefore the definition of commercial scale is supposed to be the same (LG Köln, 30.04.2009 - Az. 9 OH 388/09).

[114] LG Köln, 5.9.2008 - Az. 28 AR 6/08.

[115] LG Bielefeld, 11.9.2008 - Az. 4 O 328/08.

[116] LG Oldenburg, 15.9.2008- Az. 5 O 2421/08.

[117] LG Köln, 17.12.2008 - Az. 38 OH 11/08.

[118] OLG Köln, 9.2.2009 – Az. 6 W 182/08.

[119] OLG München, 26.7.2011 - Az. 29 W 1268/11.

So decided the LG Köln[120] on 30.4.2009 that the only act of the making publicly available of a copyright protected work via file-sharing is not enough to establish commercial scale. It decided that in this case commercial scale was not given, since the release date was more than 6 month ago and due to a report of a business association the main sale time of that type of product is only 6 months. Further it was not evident that it was a still commercial successful or popular work and also the amount of showed infringements was not of such an amount that a great demand for the movies could be deduced from it.

Also on 5.10.2010 the OLG Köln[121] decided that in case of making publicly available via a P2P Network of a music album which is on the market since more than one and a half year can not be acted without further findings on the assumption of an infringement on a commercial scale.

It confirmed this view further in its decision of 30.8.2011[122], where it stated that more than 6 month after the utilization of a movie-DVD can only on the grounds of special evidence which proves the continuance of the relevant exploitation period, a commercial scale be assumed.

2.2.6. Summary:

In Germany getting customer information from an ISP on the basis of a dynamic IP address is regulated by law and has always to be examined beforehand by a judge. The judge will decide on several points: First the requestor has to prove that he has "Aktivlegitimation", which means that he is the holder of the copyright/a license and therefore is legitimated to pursue the infringer.[123] Secondly it has to be proven that the infringement is obvious. This is usually done by delivering expert opinions proving that the software used for detecting the infringement is working properly and that the IP address is the address used for the infringement at that time. The third and most important point is the question whether the infringement is done on a commercial scale. This is usually decided by the judge by assessing whether with the infringed work money can be earned. By case law it emerged that normally up until six months after the release date of the work judges always consider publishing on a file-sharing platform as an infringement on a commercial scale. After six months a commercial scale can be assumed if there is evidence which proves the continuance of the relevant exploitation period. This can for

---

[120] LG Köln, 30.4.2009 - Az. 9 OH 388/09.

[121] OLG Köln, 05.10.2010 – Az. 6 W 82/10.

[122] OLG Köln, 30.9.2011 - Az. 6 W 213/11.

[123] G.R. Wick, „*Inhalt und Grenzen des Auskunftsanspruchs gegen Zugangsanbieter – Eine Untersuchung des § 101 UrhG unter besonderer Berücksichtigung der Filesharing-Systeme*", TGRAMEDIA, Bonn 2010, p. 37.

example be if the work is still listed high in the selling charts and a further exploitation is planned.

2.3. Law in the Netherlands:

2.3.1. Private copy:

In the Netherlands the copyright is codified in the Auteurswet (Aw). Under this law the right holder has the exclusive right to decide under which circumstances the work can be made public or be copied. But there exist some exemptions of this right like the home copy exemption, press exemption, education exemption and citation right.

Due to the "privekopie-exeptie" (art. 16b Aw, private copy exception) and the "thuiskopie-exeptie" (art. 16c Aw, home copy exception) it is allowed for private persons to copy copyrighted works for their own use, without commercial intentions.[124] In case the copy has been made with a carrier which is used to play or reproduce a work (for example a CD, DVD etc.), a levy is owed to the right holder (art. 16c lid 1 Aw). The responsibility to pay the levy rests upon the manufacturer or importer of the blank carriers used for the copy (art. 16c lid 2 Aw).

2.3.2. File sharing

Different from Germany it is in the Netherlands legal to download private copies from illegal sources. The Gerechtshof 's Gravenhage confirmed the legality of private copies from an illegal source.[125] Also the ministers of justice, economics and education stated in a letter to the second chamber considering the copyright policy that the prosecution of infringements should be focused on illegal uploading, since focus on downloader would not only "require elaborate investment with limited gain" but would also be difficult for the consumer since it is not always obvious if a source is legal or not.[126]

Problems in this legal system form the P2P-networks, because users often automatically upload content for other users while they are downloading without being aware of it. Illegal uploading

[124] Excepted from this provision are buildings (art. 16b lid 6 Aw), databases (art. 16c lid 8 Aw) and computer programs (art. 45n Aw).

[125] Gerechtshof 's Gravenhage 15.11. 2010, LJN BO3982 (Producenten geluidsdrager/St. de Thuiskopie).

[126] Kamerstukken II 2007/08, 29838 nr. 6, 23.1.2008, p.9.

is civil- as well as criminally liable in the Netherlands, because it infringes the copyright.[127] The enforcement of copyright happens generally via civil procedures which is seen as the primary way to enforce. It is stated that intellectual property rights are economic property rights and the right holder can decide by himself in which cases, against whom and in which way he wants to enforce his rights.[128] Criminal law is normally only used in cases of commercial acting infringers or in case of endangerment of public health or public safety.[129]

2.3.3. Information from an ISP based on an IP address:

In the Netherlands no special law sees upon the obligation of ISPs to give information in civil cases to requesters. Different laws are applicable for the question if the ISP has to provide the identity information of the infringer. The provider can for example based on art. 6:162 BW (wrongful act, "onrechtmatige daad") be obliged to give the information, while based on art. 8 sub f jo art. 49 "Wet bescherming persongegevens" (Wbp) it can be argued that the provider is not allowed to give the information.[130]

2.3.4. Data retention:

In the Netherlands the Directive 2006/24/EC got implemented by the "Wet bewaarplicht telecomgegevens"[131] which amended the Telecommunication law ("Telecommunicatiewet") and the law on economic crimes ("Wet op de economische delicten"). The law got accepted by the Tweede Kamer on 22 may 2008 and on 7 July 2009 by the Eerste Kamer. The approval of the Eerste Kamer was gained after the minister announced to change the retention time of internet data by law down to 6 months. The law got in force on 1 September 2009.[132] The law

---

[127] A. Huygen a.o., "Ups and downs -*Economische en culturele gevolgen van file sharing voor muziek, film en games",* TNO-rapport 34782, 12 january 2009, p. 55.

[128] Kamerstukken II 2005/06, 30392, nr. 6, 29.5.2006, p. 4.

[129] B.W.Schermer, M.Wubben, "*Feiten om te delen – digitale contentdistributie in Nederland*", Considerati, May 2011, p. 124.

[130] Hoge Raad, 5.11.2005, C04/234HR, LJN: AU4019. (Lycos/Pessers).

[131] *Wet van 18 juli 2009 tot wijziging van de Telecommunicatiewet en de Wet op de economische delicten in verband met de implementatie van Richtlijn 2006/24/EG van het Europees Parlement en de Raad van de Europese Unie betreffende de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare elektronische communicatiediensten en tot wijziging van Richtlijn 2002/58/EG* (Wet bewaarplicht telecommunicatiegegevens), Staatsblad 333, 30.7.2009.

[132] http://www.eerstekamer.nl/wetsvoorstel/31145_wet_bewaarplicht; Law can be found in Staatsblad 333 of 30 July 2009, the announcement in Staatsblad 360 of 28.8.2009.

to change the retention time of internet data got accepted on 21 June 2011 in the Tweede Kamer and on 5 July 2011 in the Eerste Kamer and came into force on 16 July 2011.[133]

2.3.4.1. Can information retained under the data retention law be accessed?

Only criminal enforcement authorities and the general intelligence and security service are allowed to access the data retained under the data retention directive. The minister of justice explicitly stated that police and justice only have access to the retained data in cases of severe crimes, but that copyright infringements can not be considered that kind of crimes.[134] Upon request gave an ISP the answer that rightful civil requests are responded with information from the customer data base. Information retained for data retention law is not used for this purpose.

2.3.4.2. Normal length of data retention for copyright purposes?

The normal length of data retention for copyright purposes depends on the ISP. If the ISP assigns static IP addresses, the information is available until the customer changes the provider. In case of dynamic IP addresses it depends on the decision of the ISP how long the information is needed.

2.3.5. Case law:

The current used way of obtaining the user information behind the IP address developed by case law. On 25 April 2002 the Rechtbank Amsterdam[135] decided that a website with information about how to disorganize the train traffic is clearly unlawful and therefore the ISP has to block the website and give information about the holder of the website, but not about the visitors of the website. The Hof Amsterdam confirmed this decision.[136]

On 9 July 2002 the Rechtbank Utrecht[137] decided that in the case of an infringer who sold under an e-mail address illegal copies of Teleatlas the ISP did not had to give the information, since Teleatlas did not try enough to obtain the information in other, less intrusive ways.

---

[133] Wet van 6 juli 2011 tot wijziging van de Telecommunicatiewet in verband met de aanpassing van de bewaartermijn voor telecommunicatiegegevens met betrekking tot internettoegang, e-mail over het internet en internettelefonie", Staatsblad 350, 15.7.2011.

[134] Kamerstukken II, 2007/08, 31 145, nr. 9, 9.1.2008, point 3.2.

[135] Rb Amsterdam 25.4.2002, KG 02/790 OdC (DB-XS4ALL).

[136] Hof Amsterdam 7.11. 2002, 762/02 SKG (XS4ALL-DB).

[137] Rb Utrecht 9.7.2002 146580/KG ZA 02-563 (Tele Atlas – Planet Media).

On 12 July 2005 the Rechtbank Utrecht [138]decided in the case of BREIN (a Dutch organization to enforce copyrights) against several ISPs that in principle a civil court is allowed to rule that the information has to be provided, but in this case the ISPs did not have to reveal the information, since BREIN obtained the IP addresses via an American examination office. Since IP addresses are considered personal data in the sense of art. 1 sub a Wbp, the processing of it by an American company was not lawfully considering the European data protection laws.

On 25 November 2005, the Hoge Raad decided in Lycos vs. Pessers[139] that regarding the obligation of an ISP to give a right holder the information about name and address of a customer a four step test can be used:

1. It must be reasonable provided that the possibility that the information, considered in itself, illegal and harmful to the third party is sufficiently probable
2. The third party has a true interest ("reëel belang") in obtaining the information
3. It is most likely that in this case no other, less intruding, possibility exists to get the information
4. By weighing the interests of the third party, the ISP and the website owner (as far as possible) the interest of the third prevails.

In 2006 a judge in the case BREIN vs. Chello[140] did not explicitly use this four step test, but reasoned that an ISP may in certain circumstances be obliged to provide the requested data to the right holders (or their representatives). These circumstances are that first, it is sufficient probable that there have been infringing (unlawful) actions of the subscribers, and second, it is beyond reasonable doubt that the person(s) whose identifying information is made available are the person(s) who are guilty for the infringement. In that case, it is possible that the privacy interests of those involved in maintaining the confidentiality of their data must yield to the interests of right holders to act against the unlawful activities.

In 2007 the Rechtbank 's Gravenhage[141] and the Rechtbank Amsterdam[142] decided in summary proceedings of website owners on whose website copyright infringing torrentfiles where downloadable that the owner of the website did act unlawful because he facilitates

[138] Rb Utrecht 12.7. 2005 194741/KGZA 05-462/BL/EV (BREIN-ISPs).

[139] Hoge Raad, 5.11.2005, C04/234HR, LJN: AU4019 (Lycos/Pessers).

[140] Rb Amsterdan, 24.8.2006, 345291 / KG 06-1112 AB, LJN: AY6903.

[141] Rb 's Gravenhage, 5.1.2007, 27647 / KG ZA 06-1417 (BREIN-KPN).

[142] Rb Amsterdam, 21.6.2007, 369220 / KG ZA 07-840 AB/MV (BREIN-Leaseweb).

infringements of copyright. Since all requirements of Pessers/Lycos were fulfilled, the judge ordered the ISPs to submit the identity information of the website owner. The Rechtbank 's Gravenhage also decided the ISP has to cut the internet connection in case the website holder owner will put the same or a similar page online again, since the ISP was an access provider, while the Rechtbank Amsterdam decided that the website providing ISP also has to delete the website.

In 2010 the Hof Amsterdam[143] decided over the question if an ISP has an non contractual information duty regarding the information of the user of an e-mail address provided by that ISP (Ziggo). That e-mail address was used to commit copyright infringements on a video platform which was provided by the second ISP (123Video). 123Video was charged by the owner of the copyright and wanted to get the information about the infringer, who was at their platform only identified by an e-mail address, a non-identifying username and the date of birth. The court ruled in this case that the interests of Ziggo prevail, since 123Video is not able to make adequate plausible that there are no other, less infringing, possibilities to obtain the information, especially since 123Video decided to provide its website in a way that users need only an e-mail address to identify themselves.

2.3.6. Summary:

In the Netherlands downloading from an illegal source is allowed, but uploading is forbidden. There is no special law about the obligation of ISPs to give right holders the information about copyright infringers, the actual used way has emerged from case law. Based on art. 6:162 BW the ISP acts wrongful if he does not provide the information to the copyright holder if certain requirements are fulfilled. Those requirements can be described as firstly there has to be an infringement, secondly the requester has to have a real interest in obtaining the information, thirdly there has to be no other, less intruding way to obtain the information and finally by weighing of the interests of the parties the interest of the requester must prevail. Another requirement stated is that it must be beyond reasonable doubt that the person about which information is requested is the infringing person.

2.4. Comparison:

Both Germany and the Netherlands know a home copy exception in their legislation. In the Netherlands this home copy exception also covers the download from an illegal source, in Germany downloading from an illegal source is deemed to be illegal by law. Uploading is an infringement of copyright in both countries.

[143] Hof Amsterdam, 19.10.2010, 200.051.728/01 (Ziggo-123Video).

In the ECJ Case Promusicae the court stated that for Member States no obligation exists to communicate personal data in order to ensure effective protection of copyright in the context of civil proceedings. But the Member States have to interpret the directives in a way which allows a fair balance between the various fundamental rights.

In the case of Bonnier audio the ECJ decided that national legislation can allow national courts to issue an order "for disclosure of personal data, made by a person who is entitled to act, to weigh the conflicting interests involved, on the basis of the facts of each case and taking due account of the requirement of the principle of proportionality".

In Germany the disclosure of personal data by an ISP is regulated by law. For copyright infringements it is regulated in § 101 Abs. 2 UrhG and if dynamic IP addresses are used in order to obtain the information a judge has to decide about the request. In the Netherlands there is no specific law upon this matter. An ISP can be obliged under art. 6:162 BW to provide the information considering certain by case law developed circumstances.

The requirements a German judge has to consider are 1. the requestor is legitimated to pursue the infringer, 2. the infringement is obvious, 3. the infringement is done on a commercial scale.

The Dutch ISP has to consider that 1. There has to be an infringement, 2. The requester has a real interest in obtaining the information, 3. There is no other less intruding way to obtain the information, 4. By weighing the interests of the parties the interest of the requester must prevail. Another stated requirement is that it must be beyond reasonable doubt that the person about who information is requested is the infringing person.

The requirements are comparable, the fact that there has to be an infringement has to occur in both countries, without it no reason nor legitimation to act exists. A requester further can only have real interest in obtaining the information in case of a copyright infringement if he is either the right holder or has a license which has been infringed, and is therefore legitimated to pursue the infringer. In Germany it is not necessary that the person about which information is requested has to be the infringing person, only the fact that the internet access has been used for an infringement is already enough to assume at least secondary liability ("Störer-Haftung"). Also it is stated that it would be impossible for a requester to prove that the person which information is requested is the infringing person since at that point of time it is not possible to know who the person is. But the German requirement of obviousness states that for an infringement to be obvious it has to be so unambiguous that an unjustified burden on third parties seems to be impossible. This can be compared to the Dutch requirement that the information requested is of the infringing person.

The main differences in the Dutch and the German weighing are that in Germany the requirement of commercial scale needs to be fulfilled, while in the Netherlands it is important

that there is no other, less infringing way to obtain the information and the interests of the parties must be weighed. For assuming a commercial scale the main question is whether money can be generated out of the copyright. By case law it developed that this is usually assumed if the release date in Germany of the work is less than 6 month ago, or after that time frame if there is evidence which proves the continuance of the relevant exploitation period. Evidence could be that the work is still listed high in the selling charts or a further exploitation is planned. This is a way to find out whether the (monetary) interest of the copyright holder is grave enough to qualify a restriction of the right to privacy. In the Netherlands it is explicitly mentioned that interests of the parties have to be weighted, but the exact criteria how this should be done are not expressed. The requirement of no existing less infringing way does not exist in Germany

This, and the fact that in the Netherlands the ISP has to decide upon these questions while in Germany it is the duty of the judge, are the main legal differences between Germany and the Netherlands. A factual difference is that at the moment in Germany right holders have usually only a maximum of 7 days to raise their claim, since after 7 days the information is often erased by the ISPs.

Which way then protects privacy better? Since judges are more trained to decide upon those legal questions than ISPs whose main sphere of activity is in a different field, it is likely that the judges can do a better weighing of all interests at stake. Further are in Germany the grounds on which the interest of the parties have to be weighed are defined by case law. For ISPs this decision is quite difficult especially since a wrong decision could result in liability of the ISP, it is more likely that the judge will protect the privacy of the end user better. How the factual situation looks like will be examined in chapter 3.

Chapter 3:

3.1. Survey:

The intention of this chapter is to find out about how the different systems of the Netherlands and Germany work in practice/reality. It was not possible to do a real quantitative analysis, since the amount of responses especially from the access providers was not sufficient, while a questionnaire to all ISPs in a country was not a valid possibility.

In the Netherlands only one provider answered to the request of information with the information that they almost never have requests of copyright holders for identity information of users for copyright infringements.

The response of Stichting BREIN, the "joint anti-piracy program of authors, artists, publishers, producers and distributors of music, film, games, interactive software and books in the Netherlands"[144] was also that in 2011 no requests for individual user information were made towards access providers. Only hosting providers and payment processors were asked for the information of administrators of illegal sites. The amount of those requests was around 60 in 2011.

In Germany no access provider wanted to give figures, but I was informed that this kind of information is given to the ISP association "eco - Verband der deutschen Internetwirtschaft e.V." , which officially recorded an amount of around 300.000 requests for IP addresses per month[145], and estimated that around 1.500 rulings per month are presented to the companies. Also the courts located at the head office of the four biggest access providers Telekom, 1&1, Vodafone and O2/Alice[146], which are due to § 105 UrhG, the "Rechtsverordnungen" of the federal states and the decision of the OLG Düsseldorf[147], usually the responsible courts for § 101 Abs. 9 UrhG requests were asked for information. These are the LG Köln (Telekom Seat Köln), the LG Frankenthal (1&1 Seat Montabaur), the LG Düsseldorf (Vodafone Seat: Düsseldorf) and the LG München (o2/Alice: Telefonica Seat: München).

LG Frankenthal gave the information that no official statistic exists, but that the tendency since the introduction of the law in September 2008 is that the amount of cases is falling, and estimates that the amount of cases was in 2008 around 30, in 2009 around 20 and less than 10 cases in 2010.

The LG Düsseldorf gave the information that before 2010 the requests were not recorded, in 2010 it was around 14 cases, in 2011 around 17 and in 2012 up until now 1 case.

The LG München also had no separate statistics on this purpose, extrapolated from the amount of one of the chambers from 2011 the amount of requests for the whole court would be around 5.980 in a year.

The usual explanation given by the courts for the low amount of requests was, that a concentration started to occur at the LG Köln, since it is responsible for the biggest access

---

[144] Stichting BREIN, "The BREIN Foundation", <http://www.anti-piracy.nl/english.php>.

[145] Eco – Verband der deutschen Internetwirtschaft e.V., „300.000 Adressen pro Monat: erfolgreicher Kampf gegen illegale Downloads", Pressemeldung 31.5.2011, <http://www.eco.de/2011/pressemeldungen/300-000-adressen-pro-monat-erfolgreicher-kampf-gegen-illegale-downloads.html>.

[146] Telekom: 45,4%; 1&1: 11,9%; Vodafone: 12,8%; O2/Alice:9,7% : Marktanteile der führenden Breitband-Anbieter in Deutschland Q3 2011 (http://www.dslweb.de/dsl-marktuebersicht.php).

[147] OLG Düsseldorf, 8.12.2008 – Az. I-20 W 130/08.

provider, Deutsche Telekom. The LG Köln gave the information that in 2009 the amount of requests was around 430 per month, in 2010 around 979 per month and in 2011 around 749 per month, the highest amount of requests occurred in March 2010 with an amount of 1300. At the moment it seems that the trend levels off at an amount of around 700 requests per month.

The difference between the amount given by eco e.V. and the amount given by the courts can be explained by the fact that not all courts were asked for information, whereby the numbers of eco also include requests at other ISPs than access providers and the fact that one request at a court often includes several hundred up until thousand IP addresses.

Even though these results are not enough to make a quantitative analysis, the difference in the amount of requests in the Netherlands, which tends to be almost zero and the amount of requests in Germany, which is significantly higher is very obvious.

There are several possible explanations for this phenomenon.

3.2. Possible explanations for the difference:

3.2.1. No download prohibition in the Netherlands:

The first and most obvious explanation for the difference of the amount of requests between Germany and the Netherlands is the fact that in the Netherlands downloading is not prohibited. But even though it seems on the first sight to completely explain the difference, there are some remarks to this. So is it in most P2P systems normal to up- and download at the same time.[148] Even though it is sometimes possible to turn off this function, a lot of users are unaware of it. Therefore the amount of requests for information of users uploading copyright infringing materials could be expected to be higher than the real amount seems to be. This is very likely since also in Germany most procedures of § 101 Abs. 9 UrhG are based on illegal uploading which is an infringements of § 19a UrhG.[149]

On 11 April 2011 State secretary of Safety and Justice ("veiligheid en justitie") Teeven presented the "Speerpuntenbrief auteursrecht 20©20" to the Tweede Kamer. In this letter the starting points of the future copyright policy of the government are described. One important

[148] A. Ringnalda, M. Elferink & M. de Cock Buning, "*Auteursrechtinbreuk door P2P filesharing - Regelgeving in Duitsland, Frankrijk en Engeland nader onderzocht*", Centrum voor Intellectueel Eigendomsrecht, 10 July 2009, p. 20.

[149] T. Kreutzer, "*Limitations of the private copying exception: miracle cure or dead end? – A review from the perspective of German copyright law*"; AMI 2011 nr. 5, p. 162.

point in the context of this thesis is point three, since it considers abolishing the extensive interpretation of the home copy exception by defining downloading from an illegal source as to be illegal.[150] It states that in this context the levy system should be abolished too, since it was a system to compensate copyright holders for illegal copies made under the home copy exception.[151] Further it states that the focus should be on websites and big infringers, no attention should be given to consumers that up- and download on a limited scale. The reason given is that it would result in an legal inequality since within this sphere not everybody can be approached. Also there should legal warrants be introduced to make sure that right holders can't enforce to get information about this kind of consumers. Information about hem may only be given in case a judge decided that somebody infringed copyright on a large extend and if it is not possible to approach the website administrator or hosting provider.[152] Up until now it is in the Netherlands still legal to download, but maybe in future this will change.[153]

3.2.2. System of "Abmahnungen" in Germany:

An "Abmahnung" in Germany is a special kind of cease and desist letter, which is used to call the attention of the infringer on his infringement and to request him to cease and desist. The infringer has to give a declaration of discontinuance with a penalty clause ("strafbewehrte Unterlassungserklärung"), the purpose of an "Abmahnung" is to avoid time-consuming and costly court proceedings.

There are no formal requirements on the form of an "Abmahnung", but it is necessary that the claimant demands a declaration of discontinuance with a penalty clause from the infringer to avoid court proceeding.[154] For that the "Abmahnung" needs to include information about the right to sue, the person which is sued, the concrete real circumstances out of which the right of injunctive relief ("Unterlassungsanspruch") results, as well as the threat of legal action.[155] The

---

[150] Kamerstukken II 2010/11, 29 838, nr. 29 ('Speerpuntenbrief Auteursrecht'), 13.4.2011, p. 10.

[151] Kamerstukken II 2010/11, 29 838, nr. 29 ('Speerpuntenbrief Auteursrecht'), 13.4.2011, p. 12.

[152] Kamerstukken II 2010/11, 29 838, nr. 29 ('Speerpuntenbrief Auteursrecht'), 13.4.2011, p. 9.

[153] See for the actual status: https://zoek.officielebekendmakingen.nl/dossier/29838 ; http://www.eerstekamer.nl/kamerstukdossier/auteursrechtbeleid.

[154] P. Nümann and Dr. M.A. Mayer, "*Rechtfertigung und Kritik von Massenabmahnungen gegen Urheberrechtsverletzungen in Filesharing-Netzwerken*", ZUM 2012, p. 323.

[155] A.A. Wandtke, W. Bullinger, "*Urheberrecht*", 3. Auflage 2009, UrhG § 97 a Abmahnung, Rn 6..

costs of "Abmahnung" and the subsequently court procedure has the claimant to bear, but he can ask for compensation of the expenses.[156]

On the occasion of the implementation of the enforcement directive 2004/48/EC, § 97a UrhG was introduced to regulate the "Abmahnung" in the sphere of copyright. This was especially to prevent the malpractice of attorneys to use the costs of an "Abmahnung" as additional source of income.[157] The legislator stated in its first draft of the law that the "Abmahnung" is an important part of the system, developed in the praxis and by case law, to solve conflicts without needing a court procedure.[158] To balance the interests of all parties the legislator wanted to limit the payment to 50 euro (in the final version it became 100 euro) for a first "Abmahnung" in simple cases, if the infringement has not been committed in course of business. Simple is defined as a routine case which can be handled without much effort and course of business is defined extensively as every commercial act with the goal to improve own or somebody else's business purpose.[159] The amount of the payment includes taxes as well as expenses like postal charges, but necessary expenses for the investigation of the infringer behind an IP address are not included.[160] The limitation did not work in practice, since usually the cases were not considered simple by the lawyers and course of business was defined very broad.

In individual cases the "Abmahnung" is a good choice, but the question arises if massively sending "Abmahnungen" is sensible and legitimate in case of massive infringements.[161]

The instrument of the "Abmahnung" is seen as an important one for asserting legal rights. But also, especially in the field of copyright related "Abmahnung", critic has arisen that it is used with the only goal to make money, not to enforce the law. Holger Bleich for example states in

---

[156] § 97a UrhG.

[157] C. Santangelo, "*Der urheberrechtliche Schutz digitaler Werke – eine vergleichende Untersuchung der Schutz- und Sanktionsmaßnahmen in deutschen, italienischen und englischen Recht*"; Max-Planck-Gesellschaft zur Förderung der Wissenschaft e.V., Freiburg i. Br., 2011, p. 63.

[158] Bundesrat, *Gesetzentwurf der Bundesregierung*, Drucksache 64/07, 26.1.2007, s. 115.

[159] Bundesrat, *Gesetzentwurf der Bundesregierung*, Drucksache 64/07, 26.1.2007, s. 116.

[160] Bundesrat, *Gesetzentwurf der Bundesregierung*, Drucksache 64/07, 26.1.2007, s. 116.

[161] P. Nümann and Dr. M.A. Mayer, "*Rechtfertigung und Kritik von Massenabmahnungen gegen Urheberrechtsverletzungen in Filesharing-Netzwerken*", ZUM 2012, p. 323.

his article "Die Abmahn-Industrie"[162] that a whole exploitation chain has been built around the system of Abmahnungen: copyright holders provide companies with the names of their copyright protected works, the companies do the research and find evidence, the lawyers send the Abmahnungen. Compensation for damages and license fees are partly passed back to the copyright holders. In the article a model calculation is explained which states that the copyright holder receives from the company 90 euro of the 450 euro asked from the infringer. Considering a 60 Cent net profit out of a legal download, the profit of an illegal "abgemahnter" download is 150 times higher, which would mean it is more profitable for copyright holders to send cease and desist letters than to sell their products legally.[163] He states further that the focus of these companies on ISPs depends on the length of time they detain their data (since data retained under the data retention law can not be used for civil enforcement). The Telekom is the biggest telecommunications provider for private individuals and saves the information for 7 days for invoicing reasons. This is the reason why it is in the focus of the copyright holders and why the Landgericht Köln has been so flooded with requests.

But there are others who stand more positive towards "Abmahnungen". So argues for example Nümann in his article that the fact that big amounts of similar "Abmahnungen" are sent is not an indication for abuse of rights, since in the case of file sharing a lot of similar infringements are pursued, which makes it only normal that a the "Abmahnungen" are in big amounts and similar.[164] He states further that it would be an abuse of right if the prosecution is only done by attorneys with the intention of gaining money without any interest of the copy right holder, but it is unreasonable to interpret the interest of the copyright holder in reimbursement of his costs as to be an abuse of his right.

Adolphsen criticizes in his article the fact that those companies specialized in litigation of copyright infringement via file-sharing often try to enforce claims on their own behalf.[165] To be able to do this they let the copyright holder grant them a license for making public of the copyrighted work in file-sharing networks in the internet, which is in his opinion legally not allowed since the making public in file-sharing networks is not an autonomous exploitation

---

[162] H. Bleich, "*Die Abmahn-Industrie – Wie mit dem Missbrauch des Urheberrechts Kasse gemacht wird*", C't 2010, Heft 1, p. 154 – 157.

[163] Calculation based on a leaked fax of the company Digiprotect, see J. Boie, „Geschäftsmodell Abmahnung", Süddeutsche Zeitung, 27. 2. 2010, <http://www.suedeutsche.de/digital/illegale-downloads-geschaeftsmodell-abmahnung-1.8519>.

[164] P. Nümann and Dr. M.A. Mayer, "*Rechtfertigung und Kritik von Massenabmahnungen gegen Urheberrechtsverletzungen in Filesharing-Netzwerken*", ZUM 2012, p. 328.

[165] Adolphsen, Mayer, Möller: „*Massenabmahnungen im Urheberrecht – Ein Geschäftsmodell auf dem Prüfstand*", NJOZ 2010, p. 2394.

method in the sense of § 31 I UrhG and the given rights are only used for enforce the rights, not to use them, which is why these companies have no protection-worthy self-interest.[166] Another way he describes is acting on behalf of others, which would give the company the status of a collecting society. For obtaining this status as trustee they would need the permission of the Patent office (§ 1 UrhWG).[167]

Due to this development, the ministry of justice considers to take actions against the current situation.[168] Mid April 2012 a first draft by the ministry of justice of a law against dubious business practices was leaked.[169] As reason for this draft has been stated in the document that "A lawyer business models should be stopped in which the mass of "Abmahnungen" of Internet users for copyright violations is operated for profit optimization, and mainly serves to generate entitlement to compensation for expenses or prosecution costs against the infringer. It is detrimental to the right holders and the legitimacy of the enforcement of their right, if such business models bring into discredit the in principle and also in other areas proven and effective institute of "Abmahnung" due to the fact that it moves the original purpose of an "Abmahnung", the removal and omission of an infringement, in the background."[170] It states further that the complaints increase about mass-"Abmahnungen" which are based completely on text modules and made without individual review while holding claims of on average 700 Euro. These amounts are the main reason for the complaints. The amount of the claim is found improperly since the for the biggest part automated procedure. In the draft is acknowledged that no official statistics of the amount of "Abmahnungen" exist, but according to the data collection of

[166] Adolphsen, Mayer, Möller: „*Massenabmahnungen im Urheberrecht – Ein Geschäftsmodell auf dem Prüfstand*", NJOZ 2010, p 2398.

[167] Adolphsen, Mayer, Möller: „*Massenabmahnungen im Urheberrecht – Ein Geschäftsmodell auf dem Prüfstand*", NJOZ 2010, p. 2399.

[168] Bundesministerium der Justiz, "Besserer Schutz gegen überzogene Abmahnungen", Nachrichten 3.11.2011, <http://www.bmj.de/SharedDocs/Kurzmeldungen/DE/2011/20111103_Besserer_Schutz_gegen_ueberzogene_Abmahnungen.html>.

[169] Bundesministerium der Justiz, "Entwurf eines Gesetzes gegen unseriöse Geschäftspraktiken", Referentenentwurf, 12.3.2012, <http://www.textintern.de/Bilder/Referentenentwurf.pdf>, the authenticity of the document was confirmed by the Ministry of Justice after inquiry of Heise online: Dr. Noogie C. Kaufmann, "'Geleakter' Gesetzentwurf: Maßnahmen gegen Abmahnmissbrauch", Heise online, 17.4.2012, <http://www.heise.de/newsticker/meldung/Geleakter-Gesetzentwurf-Massnahmen-gegen-Abmahnmissbrauch-1540816.html> / < http://heise.de/-1540816>.

[170] Referentenentwurf des Bundesministeriums der Justiz, "Entwurf eines Gesetzes gegen unseriöse Geschäftspraktiken", Bearbeitungsstand: 12.03.2012 13:48 Uhr, p. 17.

the "Verein gegen den Abmahnwahn e.V."[171] more than 218000 "Abmahnungen" have been sent in the year 2011 with a sum of total receivables of around 165 million euro and an average payer quota of around 40%.[172] In case of refusal of payment is often stated that further costs will be incurred which is a reason why a lot people pay. The asserted costs on the other hand are often not yet brought to the account of the copyright holder, which means that the receiver of the "Abmahnung" are billed for costs of the right holder which at the time of the "Abmahnung" did not (yet) arise. To change this situation the draft proposes to change § 49 GKG ("Gerichtskostengesetz") in a way that in case of copyright infringements the sum in dispute ("Streitwert"[173]) for an omission will be 500 Euro, if the defendant is a natural person which used the copyright protected works not for commercial activities and has not already been bound to omission due to a contract, a final court decision or an injunction. Additionally the position of a person which received an abusive "Abmahnung" should be strengthened by introduction of a counterclaim for reimbursement of expenses for his legal defense.[174]

The advantage of the system of "Abmahnungen" in Germany is that "Abmahnungen" are an easy and non-costly way to put the attention of the infringer on his infringement and to request him to cease and desist. Time-consuming and costly court proceedings can be avoided and legal rights are asserted. By using "Abmahnungen" often competitors control each other on the obedience of the legal rules, for example in the field of web shops. The same can be said for copyright holders who have with the "Abmahnungen" a very useful instrument to ensure their rights.

The disadvantage of the system is the fact that it is used extensively especially in the field of small private infringements of copyright law. In order to get the addresses of the infringers a big amount of requests for private information at ISPs occur. The problem is that the possibility of asking reimbursement of costs can form a perverse incentive to use this on a large scale in order to make profit. But it is difficult to decide who has a real interest and who is only looking for financial gain, since it is not possible to know about the exact agreement made between the right holder and his lawyer. Without insight in the underlying reasons for the "Abmahnungen" it

---

[171] Verein zur Hilfe und Unterstützung gegen den Abmahnwahn e.V., „Filesharing Abmahnwesen Deutschland Jahresstatistik 2011", 10.2.2012., <http://www.verein-gegen-den-abmahnwahn.de/zentrale/download/statistiken/2011/jahresbilanz_2011.html>.

[172] Referentenentwurf des Bundesministeriums der Justiz, "Entwurf eines Gesetzes gegen unseriöse Geschäftspraktiken", Bearbeitungsstand: 12.03.2012 13:48 Uhr, p. 17.

[173] In Germany the sum in dispute is used to set the fees of a lawyer, therefore if the sum in dispute is lower also the fee of the lawyer is lowered.

[174] Referentenentwurf des Bundesministeriums der Justiz, "Entwurf eines Gesetzes gegen unseriöse Geschäftspraktiken", Bearbeitungsstand: 12.03.2012 13:48 Uhr, p. 21.

is only possible to limit the profit which can be gained, which is also the approach of the draft of the ministry of justice. The disadvantage of this approach is that right holders and their lawyers who have an honest interest and put effort in their case are at a disadvantage since they will have to bear a big part of the costs, while it is theoretically for the real mass sending lawyers still possible to gain some profit since the work for making similar "Abmahnungen" is not so high that still profit can be made if enough "Abmahnungen" are sent.[175] These practices are probably responsible for the high amount of requests in Germany. Another option considered is the introduction of a counterclaim for the receiver of an "Abmahnung" to strengthen his position compared to the right holder. [176] The question is whether it will be used by users since the whole business concept of unrightfully "Abmahnungen" is based on the fact that many people rather pay than start a costly court procedure.

3.2.3. Notice and Takedown procedure in the Netherlands:

In the Netherlands the Notice and Takedown (NTD) procedure is the primary used way to handle small copyright infringements. This is not a by law prescribed procedure but a procedure which is self-imposed by the intermediaries by a code of conduct.

The general Notice-and-Take-Down Code of Conduct was created[177] as a voluntary agreement between law enforcement agencies and Dutch ISPs under lead of the NICC[178] on how to deal with allegedly illegal content.[179]

On 9 October 2008 the final version was presented to the minister of Foreign Trade Frank Heemskerk.[180] On the basis of this official NTD Code ISPConnect, one of the initiators of it, created a procedure.[181] Finally most ISPs have their own procedure, based on these models.

---

[175] J. Faustmann, "*Abmahnpauschalen, gesetzliche Streitwertvorgaben und sonstiger Aktionismus*", MMR 2011, 773.

[176] Referentenentwurf des Bundesministeriums der Justiz, "Entwurf eines Gesetzes gegen unseriöse Geschäftspraktiken", Bearbeitungsstand: 12.03.2012 13:48 Uhr, p. 18.

[177] Some ISPs had already before NTD procedures, for example XS4ALL since February 2007, see also Rb 's Gravenhage 5 January 2007, 276747/KGZA06-1417.

[178] "Nationale Infrastructuur ter bestrijding van Cybercrime"; Platform voor Cybersecurity, <https://www.cpni.nl/informatieknooppunt/de-nationale-infrastructuur-ter-bestrijding-van-cybercrime-nicc>. The secretariat of the workgroup Notice and Takedown was placed over to ECP-EPN in January 2009, ECP Platform voor de InformatieSamenleving, "Werkgroep Notice and Takedown", <http://www.ecp-epn.nl/werkgroep-notice-and-takedown>.

[179] P. Bernt Hugenholtz, "Codes of Conduct and Copyright; Enforcement in Cyberspace", in I. A. Stamatoudi (red.), "*Copyright Enforcement and the Internet*", Alphen aan de Rijn: Kluwer Law International 2010, p. 306.

A Notice and Takedown procedure commonly follows these steps:

1. A report has to be given to the ISP. This is often done via the website of the ISP. The report usually includes:
    - The name, address, e-mail address and phone number of the notifier.
    - An URL or other description of the (alleged) infringing material.
    - The requested action (blocking of the material and/or providing of the information of the infringer)
    - The reason for the complaint (infringement of copyright etc.)
    - Further information over the complaint.
    - Information whether there was an attempt to reach the provider of the (alleged) infringing material, and if so which reasons were given not to take action.
    - A declaration that the information provided in the report is truthful and that the notifier shall reimburse all damages arising from unjust information provided.
    - In case of infringement of a right the notifier also must state that he is right holder or entitled to act in the name of the right holder.
    - In case of urgency a motivation the reasons for urgency
    - Information over the procedure: Within how many days the complaint will be processed, under circumstances with the help of legal counsels and that only complete and truthful reports can be processed.
2. The ISP sends the complaint to the uploader and gives him a set time to react.
    a. If the uploader agrees with the complaint (and takes off the infringing material/gives his information), the complaint is cleared.
    b. If the uploader does not react or does not agree, the ISP acts in the following ways:
        i. If the ISP considers the complaint legitimate, he blocks/takes down the content. If he also considers the interest of the notifier real (“reëel belang"), then he gives the identity information. The uploader will be informed about this decision.
        ii. If the ISP considers the complaint not legitimate, or that the notifier has no real interest in the identification of the uploader, he informs the notifier motivated about his decision.

---

[180] Internet Society, “Gedragscode Notice and Take Down geode stap”, <http://isoc.nl/info/nieuws/2008-noticeandtakedown.htm>.

[181] Vereniging ISPConnect Nederland, “ISPConnect Notice & Takedown procedure”, <http://www.ispconnect.nl/ntd-procedure>.

The advantage of such self imposed procedures is the fact that they are made by private actors concerned with the topic, what results in norms which are fit better to the needs of the industry than imposed rules would. It is faster than legislation processes and more easily revised which makes it especially useful for fast changing domains like the internet.[182] Hugenholtz states that "Moreover, self-regulatory codes may provide for more effective and expedient mechanisms of enforcement than statutory law, especially in fields such as intellectual property law that are rarely enforced by the application of criminal law, or suffer from an overworked judiciary."[183]

But there are also some disadvantages to this type of self-regulation. These are for example legal uncertainty and the fact that the codes are non-binding.[184] But probably the biggest disadvantage of the NTD procedures is the fact that they directly affect fundamental rights and freedoms of consumers, but are often made in a nontransparent way without participation of those who are in the end affected in their rights.[185] Hugenholtz states that "To avoid that intermediaries become self-appointed censors or tread on the rights of privacy of their end users, self-regulation must be firmly integrated into a legislative framework that guarantees stringent governmental or judiciary oversight."[186]

3.3. Conclusion:

It has been shown that the amount of requests for information in Germany and the Netherlands differ significantly. While in Germany the ISPs face every month around 300.000 requests, the amount is in the Netherlands negligible. This prompts two questions: Is under these circumstances the protection of privacy is effective and what is the reason for the difference in amount of requests.

---

[182] P. Bernt Hugenholtz, "Codes of Conduct and Copyright; Enforcement in Cyberspace",in I. A. Stamatoudi (red.), "*Copyright Enforcement and the Internet*", Alphen aan de Rijn: Kluwer Law International 2010, p. 306.

[183] P. Bernt Hugenholtz, "Codes of Conduct and Copyright; Enforcement in Cyberspace",in I. A. Stamatoudi (red.), "*Copyright Enforcement and the Internet*", Alphen aan de Rijn: Kluwer Law International 2010, p. 307.

[184] P. Bernt Hugenholtz, "Codes of Conduct and Copyright; Enforcement in Cyberspace",in I. A. Stamatoudi (red.), "*Copyright Enforcement and the Internet*", Alphen aan de Rijn: Kluwer Law International 2010, p. 307.

[185] P. Bernt Hugenholtz, "Codes of Conduct and Copyright; Enforcement in Cyberspace",in I. A. Stamatoudi (red.), "*Copyright Enforcement and the Internet*", Alphen aan de Rijn: Kluwer Law International 2010, p. 308.

[186] P. Bernt Hugenholtz, "Codes of Conduct and Copyright; Enforcement in Cyberspace",in I. A. Stamatoudi (red.), "*Copyright Enforcement and the Internet*", Alphen aan de Rijn: Kluwer Law International 2010, p. 308.

Is the protection under these circumstances effective?
In Germany a request for the information behind dynamic IP addresses always has first to be considered by a judge, which is supposed to decrease the danger for privacy. But in practice a judge gets sometimes thousands of IP addresses per request and has only a short time to decide upon this question, so it is difficult to examine the rightfulness of the requests properly. The judge can only decide based on expert opinions provided by the requester that the software works right and these IP addresses are addresses of infringers. Since the request is for the access to information, the person whose information is requested has at that point of the procedure no possibility to complain or give reasons against the accessing of its information by the requester, due to the fact that neither the requester nor the person whose information is requested know at that moment whose information is inquired.

In the Netherlands on the other hand rests the decision about the rightfulness of a request on the shoulders of the ISPs. This has led to the introduction of Notice and Takedown procedures which give the ISPs the possibility to let their customers know of the supposed infringement before they under circumstances give away their information. Since the amount of requests in the Netherlands is significantly lower than in Germany it is not too burdensome for the ISPs to be the intermediary between the right holder and their customers.

But in the Netherlands it is proposed to change the current policy of home copy exception by declaring downloading from an illegal source to be illegal, like it is in Germany. In the statement is declared that no attention should be given to consumers that download on a limited scale. To keep the privacy safe a judge would have to decide if information of an infringer can be given away, whereby the decision is based on the question whether somebody infringed copyright on a large scale and if it is not possible to approach the website administrator or hosting provider.

What is the reason for this difference in amount of requests?

Assuming that in the Netherlands and in Germany the amount of copyright infringers within the population can be considered to be similar, the fact that Germany has a 5 times higher population could be a factor. But even then an amount of around 60000 requests per month could be expected for the Netherlands. Even though the responses of the ISPs and Stichting BREIN have a limited validity, there is no indication that the amount of requests in the Netherlands is that high.

One explanation could be that while it is in Germany forbidden to download from an illegal source, is it in the Netherlands allowed. But since it is within P2P networks common to download and upload simultaneously, it could be expected that in the Netherlands, even though no download prohibition exist, the amount of requests would be higher. Since this is not

the case and also in Germany most requests for § 101 Abs. 9 UrhG procedures are based on uploading as an infringement of § 19a UrhG (the right to make public) other explanations need to be found.

Germany and the Netherlands not only have different systems of handling requests for information but also different ways of enforcement. It is likely that due to these differences the amount of questions for information differs between the countries.

While the focus in the Netherlands for example of the Stichting BREIN is more set upon the big infringers and for example website administrators who facilitate copyright infringements[187], this seems to be different in Germany. A reason which is given for this is that with decentral P2P networks it is not possible to go against central facilitators, so the only way to enforce the right is to go against the masses of P2P users.[188] In Germany it is common in case of small copyright infringement not to not start court proceedings but to send cease and desist letters, the so called "Abmahnungen". In the "Abmahnung" is asked for signing a declaration which imposes fines on every future infringement, but the (supposed) infringer is also asked to pay immediately the expenses of the copyright holder. It is possible that the difference in amount of requests arose due to the possibility of asking reimbursement of payments for a "Abmahnung" in Germany, which led to a higher amount of requests than in the Netherlands.

In the Netherlands it is also possible to send a cease and desist letters.[189] For example Stichting BREIN uses an anti-piracy declaration ("Anti-Piraterij Verklaring") in which the infringer has to sign that he will in future refer from making illegal copies and in case of disobeying this after the signing of the declaration a fine of 500 Euro for every illegal copy can be imposed. But the infringer does not have to pay at that point of time, only if the infringement is repeated. This is different from the way it is done in Germany.

In principle it is not unjust to give the possibility to reclaim the costs of enforcement of the copyright holders right, since if the copyright holder is only able to protect his right by bearing

---

[187] Stichting BREIN, "Ons Beleid", <http://www.anti-piracy.nl/ons-beleid.php>.

[188] For example: P. Nümann and Dr. M.A. Mayer, "*Rechtfertigung und Kritik von Massenabmahnungen gegen Urheberrechtsverletzungen in Filesharing-Netzwerken*", ZUM 2012, p. 331; or G.R. Wick, „*Inhalt und Grenzen des Auskunftsanspruchs gegen Zugangsanbieter – Eine Untersuchung des § 101 UrhG unter besonderer Berücksichtigung der Filesharing-Systeme*", TGRAMEDIA, Bonn 2010, p.7.

[189] Stichting BREIN states in its' policy to usually solve small cases with a cease and desist letter, and only use court proceedings if the infringer refuses to sign. In case of repetition the infringer needs to pay the fine. In bigger cases compensation for damages and profit remittance are claimed. Some small cases which have only little risk of repetition are handled with an advanced notice/written warning (waarschuwingsbrief); Stichting BREIN, "Ons Beleid", <http://www.anti-piracy.nl/ons-beleid.php>.

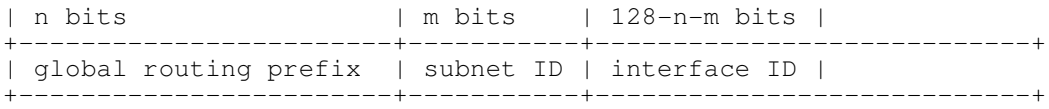
huge costs it would lead to derogation of his right. But in Germany it has led to excessive requests with a focus on end users and sometimes even people who did not infringe in person but are secondary liable as “Störer”.

Chapter 4:

4.1. Ipv6:

The problem of IPv4 is its limited address space. Due to the, at the time of development of IPv4 unexpected, big growth of the Internet and the resulting forecasted exhaustion of IPv4 addresses, IPv6 was designed. The IPv6 uses 128-bit addresses, which are expressed using hexadecimal notation (e.g. 2001:db8:85a2e:370:7334). The usage of 128-bit addresses can provide the huge amount of 2^{128} or 3.40281367 x 1038 IP addresses.

Due to the RFC 4291[190] the general format for IPv6 Global Unicast addresses is:



Source: rfc 4291 p.9.

The addresses which do not start with binary 000 have an interface ID field of 64-bit (i.e. n + m = 64)[191]

Typically the first 32 bit are assigned to the ISP by an RIR.[192] This part gets divided into subnets by the provider. A single subnet gets usually a 64 bit long prefix assigned, which forms together with a 64 bit long Interface Identifier the address.[193]

ISPs don’t need to assign a complete 64 bit-prefix, it is also enough to assign for example only 48 bit. The rest of the prefix can then be freely chosen by the user, so different subnets can get different prefixes. Only by looking at an IPv6 address it is not possible to find out how big the

[190] RFC 4291, p.9.

[191] RFC 4291, p. 10.

[192] RIPE, “IPv6 Address Allocation and Assignment Policy”; RIPE 552, May 2012, p. 6, p.7.

[193] RFC 4291, p. 10.

part is which was assigned by the provider (the global routing prefix), and how many bits the user chose himself (subnet identifier).[194]

While for IPv4 the IP addresses were allocated by host configuration protocols like DHCP, exists for IPv6 the system of IPv6 Stateless Address Autoconfiguration. This is a way how devices can automatically configure their IP address by themselves, without the need for a server.[195]

The Interface Identifier can either be generated out of the MAC-address of the Network interface card or in another way.[196] The MAC-address (Media-Access-Control-address) is the number which is assigned to network interfaces to recognize them in a network. It is allocated in the OSI model on layer two, as a sub-layer of the data link layer.

The problem of the original idea to generate the Interface identifier out of the MAC-address is that the MAC-address is a unique identifier. This has the implication that even if a person is connecting at another place, since the IP address is generated out of the MAC-address it is a unique address which stays the same. This could be a danger to privacy since the device can be recognized immediately which makes it easy to track the user. To address this problem different solutions have been considered. One of these is to not use Stateless Address Autoconfiguration but use the server-based method DHCPv6, the DHC protocol for IPv6. Another option which still enables the use of Stateless Address Autoconfiguration are privacy extensions. The idea of privacy extension was first mentioned in RFC 3041 in 2001 which was obsoleted by RFC 4941 in 2007. The privacy extensions make it possible that the interface identifier of the IP address changes randomly over time.[197] Also multiple IP addresses can be used so that for example for incoming connection requests a static IP address can be used, while for initiating communication temporary IP addresses are used.[198]

4.2. Implementation of IPv6 in Germany and the Netherlands:

The IPv6 was established between 1993 and 1998, the deployment of it started in 1999. But the rate of end users who use IPv6 is still negligible. On the World IPv6 Launch Day, 6.6.2012, around 3000 content provider and hoster changed their systems so that they can be used

---

[194] B. Freund, C. Schnabel, *„Bedeutet IPv6 das Ende der Anonymität im Internet? Technische Grundlagen und rechtliche Beurteilung des neuen Internet-Protokolls“*, MMR 2011, p. 496.

[195] First described in RFC 4862.

[196] RFC 4291, p. 20 (appendix A).

[197] RFC 4941, p. 1.

[198] RFC 4941, p.8.

parallel for IPv4 and IPv6.[199] Germany and the Netherlands both requested plenty of IPv6 addresses. Even though TNO states that the factual roll out can only be considered average since only a small part of the IPv6 addresses are used and the amount of IPv6 traffic is still very low.[200] The main users of IPv6 at the moment seem to be in the scientific sphere and within sectors which are intensively engaged with Internet. The percentage of IPv6 users under consumers is lower than 1%[201] and a rise of the use of IPv6 during 2011 did not occur. An explanation is that only a small amount of products supports IPv6 and the purchasing departments of big electronic chains do not yet consider IPv6 as important.[202] It is expected that during 2012 the first consumers will be connected with IPv6, so far it is not clear until when more services and content for IPv6 will be available.[203]

In Germany the Deutsche Telekom stated that IPv6 for end users should be available until the end of 2012.[204] Up until now in Germany only three small network operators are registered as providing IPv6 and in the Netherlands two access providers (XS4ALL and SURFnet).[205]

4.3. Conclusion:

It seems that more time will need to pass until the transition to IPv6 will reach the end user. But even though the implications of this transition should be considered. One of these implications could be that without privacy extensions it would in principle be possible to identify private customer IP addresses on a large scale in WHOIS databases, since static IP addresses are often registered there with name and address. This could make it possible that neither a judge nor an

---

[199] Heise online, "World IPv6 Launch Day: Das Experiment geht weiter", 6.6.2012, <http://www.heise.de/newsticker/meldung/World-IPv6-Launch-Day-Das-Experiment-geht-weiter-1611755.html> / < http://heise.de/-1611755>.

[200] A. van der Giessen, A. van der Plas, S. van Oort, "*TNO marktrapportage June 2011*", 1.7.2011, TNO rapport 35532, p.25.

[201] M. Boen-Leo, A.Holtzer, & a.o. "*IPv6 Monitoring in Nederland: De Vierde Meting*", TNO-whitepaper, 10.11.2011, 35565, p.30.

[202] M. Boen-Leo, A.Holtzer, & a.o. "*IPv6 Monitoring in Nederland: De Vierde Meting*", TNO-whitepaper, 10.11.2011, 35565, p. 2.

[203] A. van der Giessen, A. van der Plas, S. van Oort, "*TNO marktrapportage June 2011*", 1.7.2011, TNO rapport 35532, p.25.

[204] M. Ermert, „Telekom verspricht IPv6 für Privatkunden-Anschlüsse bis Ende 2012", Heise online 6.6.2012, <http://www.heise.de/newsticker/meldung/Telekom-verspricht-IPv6-fuer-Privatkunden-Anschluesse-bis-Ende-2012-1605061.html> ; Deutsche Telekom, „Deutsche Telekom bietet anonymes Surfen mit IPv6", 23.11.2011 <http://www.telekom.com/medien/konzern/93240>.

[205] World Ipv6 Launch, "Participants", <http://www.worldipv6launch.org/participants/?q=2>.

ISP is needed in order to identify internet users. But this would also be a very grave danger to privacy and is therefore not very likely to occur. It is more likely that either the ISPs do not register these static IP addresses or that the access to the WHOIS databases are restricted for privacy reasons. It is even feared that the implementation of IPv6 could result in less accurate WHOIS databases since the ISPs are not forced to update the database anymore since they get larger blocks of IP addresses assigned which means the RIRs have less influence on the ISPs to oblige them to keep the information up to date.[206] It is also very likely that by the increasing implementation of IPv6 also the use of privacy extensions or DHCPv6 will become normal to the end user. This would not change the current situation since the requestor would still need the information of the ISP in order to identify the infringer.

But even though the transit to IPv6 is almost invisible to the normal internet user, it can have some legal implications if static IP addresses are used. This is right now already recognizable in the decision of the Federal Court of Justice on 24 January 2012 on the constitutionality of the §§ 111 till 113 of the Telekommunikationsgesetzes (TKG). [207] The court states that dynamic IP addresses fall under the scope of protection of the Art. 10 Abs. 1 GG, since they have a special closeness to concrete telecommunication procedures and Telecommunication companies need to screen the connection data of the user to identify the IP address. Static IP addresses on the other hand do not fall under this scope of protection, because the information is limited to the abstract attribution of number and subscriber.[208] The court emphasizes that the § 111 and 112 TKG are right now not disproportional, since dynamic IP addresses are not included in these laws and private users and individual customers currently usually have dynamic IP addresses assigned to them.[209] This could change with the introduction of IPv6, if static IP-addresses become standard for private users and individual customers. Since this could lead to a broad and permanent deanonymization of communication procedures in the internet, it could change the constitutional permissibility of the paragraphs. The legislator has in this case the duty to observe and amend.[210]

---

[206] D. McCullagh, "FBI, DEA warn Ipv6 could shield criminals from police", CNET 15.6.2012, <http://news.cnet.com/8301-1009_3-57453738-83/fbi-dea-warn-ipv6-could-shield-criminals-from-police/>.

[207] BVerfG, 1 BvR 1299/05 vom 24.1.2012.

[208] BVerfG, 1 BvR 1299/05 vom 24.1.2012, abs. 115 and 116.

[209] BVerfG, 1 BvR 1299/05 vom 24.1.2012, abs. 139 and 160.

[210] BVerfG, 1 BvR 1299/05 vom 24.1.2012, abs. 161.

A positive effect for copyright holders in Germany could be that with static IP addresses the retention time is as long as the customer stays with the same provider, which is an improvement of the current situation of a retention of max. 7 days.

A problem for copyright holders could form the again arising possibility of end to end communication under IPv6. This could stimulate the set up of restricted PSP networks, since it is easy to restrict the access to only certain IP addresses of friends. This could form a problem for copyright holders since it makes it more difficult to get hold of IP addresses of infringers. The currently used way to obtain IP addresses within open P2P networks would not work in these restricted networks. This would ask for other ways of enforcement of copyright, which are not known yet and could form an even greater danger for privacy, since it very likely would be necessary to get access to files on the computer in order to find out if copyrighted material has been illegally copied.

Chapter 5:

The main problem is the fact that for pursuing copyright infringements if only the IP address of the infringer is at hand, it is necessary to breach privacy in order to find out who infringed the copyright. But how should the different interests at stake be balanced? Big scale infringements with obvious commercial reason are neither in Germany nor in the Netherlands a problem, since in that case the infringement of privacy is reasonable and proportional. The decision is more difficult in case of small scale private up-/downloader. With regard to those Germany and the Netherlands follow different opinions.

The ideal situation would be if no infringements would need to be prosecuted, since in that case the problem of the opposing interests would not occur. Theoretically there are three situations in which no infringements would occur:

- Nobody *will* download/upload protected works: Then either all users would have ethical objections against infringing copyright or the prosecution would need to be so severe and the detection rate so high that the users would be too afraid to download illegal content. Problem: This would imply the abolishment of privacy since for a successful detection all users would need to be monitored. This situation is favorable for copyright holders.
- Nobody *can* download/upload protected works: This was the past situation before the development of the internet and the easier ways to share data. Nowadays for example DRM systems could theoretically make it possible. Problem: DRM has been tried, but

was up until not very successful due to the fact that DRM systems get hacked and at the same they often give disadvantages to legal buyers.
- Downloading and uploading protected works is *not illegal*: Problem: This would undermine the right of the right holders. This situation is favorable for privacy.

None of these situations do exist in reality, but they can be used to illustrate the different mentality towards copyright and privacy of Germany and the Netherlands.

Germany seems to be aiming more towards the first situation by enforcing the copyright against infringing masses, in the hope that it will discourage infringers and make them buy legal products. Germany considers the interest of the right holders as grave enough in case of private illegal filesharing to give the possibility to enforce their rights. The "Abmahnung" is the preferred way to handle private copyright infringements. This is then done on a large scale.
To keep a safeguard of the freedom of telecommunication the "Richtervorbehalt" is introduced. But it is questionable whether it provides a reasonable protection of privacy since judges have to decide on big amounts of requests.

The Netherlands preferred so far more the third situation, since it is not illegal to download and small uploaders are usually not prosecuted. In the Netherlands the infringement of private file sharers is not considered to be that grave and therefore downloading is not illegal, which makes an enforcement of copyright against downloaders impossible. The reason given for that is that prosecuting private infringers would not only "require elaborate investment with limited gain" but would also be difficult for the consumer since it is not always obvious if a source is legal or not. But the rights of the copyright holders are still tried to be protected by making uploading illegal and by this theoretically making downloading impossible if no copyrighted works are shared. The prosecution is more focused on large scale infringers whose right to privacy can easier be proportionally restricted. This could be the reason why in the Netherlands less legal warrants are installed to safeguard privacy. The judgment of the rightfulness of requests is left upon the ISPs with as guidance the by case law developed criteria. This has led in the Netherlands to the introduction of a Notice and Takedown procedure in which the customer is informed of the suspicion and can respond to it, before his information is given away. Also is probably due the policy and the non-existence of "Abmahnungen" the amount of requests manageable.

The Netherlands proposed to restrict the currently used policy and declare downloads from illegal sources as illegal. The question is, if the government does implement the projected amendment of the home copy exception, will the Dutch situation turn more into the German and will the ISPs will face a big amount of requests?

The Netherlands recognized this problem with the suggestion that a procedure should be introduced in which a judge should decide on the rightfulness of information requests.

Further does in the Netherlands the system of "Abmahnungen" not exist in the way it does in Germany. Therefore it is unlikely that in the Netherlands even with a prohibition on downloading a huge increase in requests for information will occur.
In the official reaction on the rapport which led to the proposal is stated that it should be ensured that small scale up- and downloaders won't be prosecuted. It states that

"*the criminalization and designation as unlawful of downloading from illegal sources, such as the parliamentary working group proposes, has the disadvantage that the enforcement policy could focus on the private sphere and that a form of control on the usage of internet of individuals could occur. This could lead to a decrease in public support for copyright law in general. Also could in this case the willingness of consumers to pay for digital Music of film can decrease*".[211]

This is especially interesting considering that in Germany momentarily a huge debate on copyright law is ongoing and a political party ("Piratenpartei") which main election campaign topics are the amendment of the copyright and better protection of privacy is gaining votes.

Germany can learn from the Netherlands an additional way to ensure privacy via NTD procedures. In principle is in Germany the reluctance against NTD procedures high, since it is seen as a kind of censorship of the internet. But the possibility to inform the customer about the request and give him a chance to react on it before his information is delivered to the requester is a positive result of the in the Netherlands used NTD procedure. In Germany the user mostly only gains knowledge of the fact that his information was requested when he gets an "Abmahnung". For privacy it would be beneficial if a possibility of informing the person of the request for its information before giving the information away would be implemented. A disadvantage is that the problem of the high amount of requests stays, which would put an unmanageable burden upon the ISPs. Different ways to decrease the amount of "Abmahnungen" are considered throughout the years, most recent the proposal of the German ministry of justice. The most successful way to decrease the amount of "Abmahnungen" for Germany would probably be to not enforce the copyright against small infringers like in the

[211] Kamerstukken II 2009/10, 29 838, nr. 22, 5.11.2009, p. 18. ("Het strafbaar stellen en als onrechtmatig aanmerken van *downloaden* uit illegale bron, zoals de parlementaire werkgroep voorstelt, heeft wel als nadeel dat het handhavingsbeleid zich op de privésfeer zou kunnen gaan richten en dat er een vorm van controle op het internetgebruik van particulieren zou kunnen ontstaan. Dit zou kunnen leiden tot een afname van het maatschappelijk draagvlak voor het auteursrecht in het algemeen. Ook zou in dat geval de bereidheid bij consumenten om te betalen voor digitale muziek of film kunnen verminderen").

Netherlands. But this would undermine the right of copyright holders. In the end it depends on every countries valuation of the rights which way is the most preferred.

How the future enforcement will look like will also be influenced by the implementation of IPv6. At this point of time it is not possible to assess whether the implementation of IPv6 will be beneficial for copyright holders because it will make it easier for them to get the infringers information, or will be beneficial for copyright infringers since it will make it easier for them to hide their information.

Bibliography

Literature

M. Boen-Leo, A.Holtzer, & a.o. "*IPv6 Monitoring in Nederland: De Vierde Meting*", TNO-whitepaper, 10.11.2011, 35565.

A. van der Giessen, A. van der Plas, S. van Oort, "*TNO marktrapportage June 2011*", 1.7.2011, TNO rapport 35532.

Foster Henderson: "*Understanding the Ramifications of IPv6" Ch.7 in edit. H. F. Tipton & M. Krause Nozaki "Information Security Management Handbook*", 6th edition, , volume 5, 2012 CRC Press, Boca Raton.

A. Huygen a.o., "Ups and downs -*Economische en culturele gevolgen van file sharing voor muziek, film en games",* TNO-rapport 34782, 12 january 2009.

A. Kramer, „*Zivilrechtlicher Auskunftsanspruch gegenüber Access Providern – Verpflichtung zur Herausgabe der Nutzerdaten von Urheberrechtsverletzern unter Berücksichtigung der Enforcement-Richtlinie*", Verlag Dr. Kovac, Hamburg, 2007.

C. Kuner, C. Burton, J. Hladjk, O. Proust, "*Study on Online Copyright Enforcement and Data Protection in selected Member States", for DG Internal Market of the European Commission"*, November 2009, p. 34.

OECD, "*OECD Communications Outlook 2011"*, 2011, OECD Publishing.

A. Ringnalda, M. Elferink & M. de Cock Buning, "*Auteursrechtinbreuk door P2P filesharing - Regelgeving in Duitsland, Frankrijk en Engeland nader onderzocht*", Centrum voor Intellectueel Eigendomsrecht, 10 July 2009.

RIPE, "IPv6 Address Allocation and Assignment Policy"; RIPE 552, May 2012.

C. Santangelo, "*Der urheberrechtliche Schutz digitaler Werke – eine vergleichende Untersuchung der Schutz- und Sanktionsmaßnahmen in deutschen, italienischen und englischen Recht*"; Max-Planck-Gesellschaft zur Förderung der Wissenschaft e.V., Freiburg i. Br., 2011.

L.A.R. Siemerink, "*De overeenkomst van Internet Service Providers met consumenten*", diss. Leiden: Kluwer 2007.

B.W.Schermer, M.Wubben, "*Feiten om te delen – digitale contentdistributie in Nederland*", Considerati, May 2011.

I. A. Stamatoudi (red.), "*Copyright Enforcement and the Internet*", Alphen aan de Rijn: Kluwer Law International 2010.

A.A. Wandtke, W. Bullinger, "*Urheberrecht*", 3. Auflage 2009, UrhG § 97 a Abmahnung, Rn 6.

G.R. Wick, *„Inhalt und Grenzen des Auskunftsanspruchs gegen Zugangsanbieter – Eine Untersuchung des § 101 UrhG unter besonderer Berücksichtigung der Filesharing-Systeme*", TGRAMEDIA, Bonn 2010.

Articles & Journals

Adolphsen, Mayer, Möller: *„Massenabmahnungen im Urheberrecht – Ein Geschäftsmodell auf dem Prüfstand*", NJOZ 2010, p 2398.

H. Bleich, "*Die Abmahn-Industrie – Wie mit dem Missbrauch des Urheberrechts Kasse gemacht wird*", C't 2010, Heft 1 p. 154 – 157.

C. Czychowski, J. Nordemann; "*Use of retained data and copyright law in Germany – the German data protection problem to fight internet piracy"*; E.I.P.R. 2010, 32(4), 174-177.

C. De Simone, "*Pitting Karlsruhe against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive*", German Law Journal, Vol. 11 No. 3, p.305.

B. Freund, C. Schnabel, *„Bedeutet IPv6 das Ende der Anonymität im Internet? Technische Grundlagen und rechtliche Beurteilung des neuen Internet-Protokolls*", MMR 2011, p. 496.

J. Faustmann, "*Abmahnpauschalen, gesetzliche Streitwertvorgaben und sonstiger Aktionismus*", MMR 2011, 773.

T. Hoeren, "*Anonymität im Web – Grundfragen und aktuelle Entwicklungen*", ZRP 2010, p. 253.

T. Kreutzer, "*Limitations of the private copying exception: miracle cure or dead end? – A review from the perspective of German copyright law*"; AMI 2011 nr. 5 , p. 160 – 163.

S. Larsson, "*The path dependence of European copyright*", Scripted Volume 8, Issue 1, April 2011, p. 22.

P. Nümann and Dr. M.A. Mayer, "*Rechtfertigung und Kritik von Massenabmahnungen gegen Urheberrechtsverletzungen in Filesharing-Netzwerken*", ZUM 2012, p. 323.

Jessica Wood, "*The Darknet: A Digital Copyright Revolution"*, XVI Rich. J.L. & Tech. 14 (2010), p. 17.

Request for comments

Can be looked up under http://www.ietf.org/rfc.html.

RFC 675: V. Cerf, Y. Dalal, C. Sunshine, "Specification of Internet Transmission Control Program", December 1974.

RFC 812: K. Harrenstien, "NICNAME/WHOIS", 1 March 1982.

RFC 959: J. Postel, J. Reynolds, "File Transfer Protocol (FTP)", October 1985.

RFC 2131: R. Droms, "Dynamic Host Configuration Protocol", March 1997.

RFC 3041: T. Narten, R. Draves, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", January 2001.

RFC 3233: P. Hoffman, S. Bradner, "Defining the IETF", February 2002.

RFC 4291: R. Hinden, S. Deering, "IP Version 6 Addressing Architecture", February 2006.

RFC 4862: S. Thomson, T. Narten, T. Jinmei, "IPv6 Stateless Address Autoconfiguration", September 2007.

RFC 4941: T. Narten, R. Draves, S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", September 2007.

Legislation and other authoritative sources

EU:

Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce in the Internal Market (Directive on electronic commerce) and

Directive 2001/29/EC of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society interesting.

Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector

Directive 2004/48/EC of 29 April 2004 on the enforcement of intellectual property rights (IPRED)

Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (Data Retention Directive)

Germany:

Gesetz über den Datenschutz bei Telediensten, 22.7.1997, BGBl I, S. 1870, in force since 1.8.1997. Out of force since 1.3.2007.

Zweites Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft, 26.10.2007, BGBl I S. 2513, in force since 1.1.2008.

Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007, BGBl I S. 3198, in force since 1.1.2008.

Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums, Drucksache 279/08, 02.05.2008, BGBl I, S. 1191, in force since 1.9.2008.

Bundesrat, *Gesetzentwurf der Bundesregierung*, Drucksache 64/07, 26.1.2007.

Bundesrat, *Empfehlungen der Ausschüsse*, Drucksache 64/1/07, 26.02.2007.

Bundesrat, *Stellungnahme des Bundesrates*, Drucksache 64/07 (Beschluss), 9.3.2007.

Deutscher Bundestag, *Gesetzentwurf der Bundesregierung*, BT-Drs. 16/5048, 20.4.2007.

Deutscher Bundestag, *Beschlussempfehlung und Bericht*, BT-Dr 16/6979, 7.11.2007.

Deutscher Bundestag, *Beschlussempfehlung und Bericht des Rechtsausschusses (6. Ausschuss) zu dem Gesetzentwurf der Bundesregierung*, BT-Drucksache 16/8783, 09. 04. 2008.

Referentenentwurf des Bundesministeriums der Justiz, "Entwurf eines Gesetzes gegen unseriöse Geschäftspraktiken", Bearbeitungsstand: 12.03.2012 13:48 Uhr.

Netherlands:

Wet van 18 juli 2009 tot wijziging van de Telecommunicatiewet en de Wet op de economische delicten in verband met de implementatie van Richtlijn 2006/24/EG van het Europees Parlement en de Raad van de Europese
Unie betreffende de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare elektronische communicatiediensten en tot wijziging van Richtlijn 2002/58/EG (Wet bewaarplicht telecommunicatiegegevens), Staatsblad 333, 30.7.2009.

Wet van 6 juli 2011 tot wijziging van de Telecommunicatiewet in verband met de aanpassing van de bewaartermijn voor telecommunicatiegegevens met betrekking tot internettoegang, e-mail over het internet en internettelefonie", Staatsblad 350, 15.7.2011.

Kamerstukken II 2007/08, 29838 nr. 6, 23.1.2008.

Kamerstukken II 2005/06, 30392, nr. 6, 29.5.2006.

Kamerstukken II, 2007/08, 31 145, nr. 9, 9.1.2008.

Kamerstukken II 2009/10, 29 838, nr. 22, 5.11.2009.

Kamerstukken II 2010/11, 29 838, nr. 29 ('Speerpuntenbrief Auteursrecht'), 13.4.2011.

Case Law & opinions

EU:

Case C-275/06, Productores de Música de España (Promusicae) v Telefónica de España SAU.

Case C-461/10, Bonnier Audio vs. Perfect Communication, 19 April 2012.

Opinion of Advocate General Jääskinen, Case C-461/10, 17.11.2011, 59.

Germany:

Landgericht and lower courts:
AG Darmstadt, 1.7.2005 – Az. 300 C 397/04

LG Darmstadt, 25.1.2006 – Az. 25 S 118/2005
LG Offenburg, 17.04.2008 - Az. 3 Qs 83/07
LG Frankenthal, 21.5.2008 – Az. 6 O 156/08
LG Stralsund, 11.7.2008 – Az. 26 Qs 177/08
LG Köln, 2.9.2008 - AZ. 28 AR 4/08
LG Köln, 5.9.2008 - Az. 28 AR 6/08
LG Bielefeld, 11.9.2008 - Az. 4 O 328/08
LG Oldenburg, 15.9.2008- Az. 5 O 2421/08
LG Frankenthal, 15.09.2008 - 6 Az. O 325/08
LG Köln, 17.12.2008 - Az. 38 OH 11/08
LG Hamburg, 11.03.2009 - Az. 308 O 75/09
LG Köln, 30.04.2009 - Az. 9 OH 388/09
LG München, 24.05.2011 - Az.: 21 O 9065/11

Oberlandesgericht
KG Berlin, 25.9.2006 – Az. 10 U 262/05
OLG Zweibrücken, 26.9.2008 - Az. 4 W 62/08
OLG Köln, 21.10.2008 - Az. 6 Wx 2/08
OLG Düsseldorf, 8.12.2008 – Az. I-20 W 130/08
OLG Köln, 9.2.2009 – Az. 6 W 182/08
OLG Frankfurt am Main, 12.05.2009 - Az. 11 W 21/09, MMR 2009, 542
OLG Karlsruhe, 01.09.2009 - Az. 6 W 47/09
OLG Zweibrücken, 21.09.2009 - Az. 4 W 45/09
OLG Köln, 05.10.2010 – Az. 6 W 82/10
OLG München, 26.7.2011 - Az. 29 W 1268/11
OLG Köln, 30.9.2011 - Az. 6 W 213/11
OLG Köln, 10.1.2012 – Az. 6 U 242/11

Bundesgerichtshof
BGH, 26.10.2006 – Az. III ZR 40/06 vom 26. Oktober 2006
BGH, 13.1.2011 – Az. III ZR 146/10; MMR 5/2011

Bundesverfassungsgericht
BVerfG, 2.3.2010 – Az. 1 BvR 256/08
BVerfG, 11.3.2008 – Az. 1 BvR 256/08
BVerfG, 24.1.2012 – Az. 1 BvR 1299/05

Netherlands:

Rechtbank
Rb Amsterdam 25.4.2002, KG 02/790 OdC (DB-XS4ALL).

Rb Utrecht 9.7.2002 146580/KG ZA 02-563 (Tele Atlas – Planet Media).
Rb Utrecht 12.7. 2005 194741/KG ZA 05-462/BL/EV (BREIN-ISPs).
Rb Amsterdan, 24.8.2006, 345291 / KG 06-1112 AB, LJN: AY6903.
Rb 's Gravenhage, 5.1.2007, 27647 / KG ZA 06-1417 (BREIN-KPN).
Rb Amsterdam, 21.6.2007, 369220 / KG ZA 07-840 AB/MV (BREIN-Leaseweb).

Gerechtshof
Hof Amsterdam 7.11. 2002, 762/02 SKG (XS4ALL-DB).
Hof Amsterdam, 19.10.2010, 200.051.728/01 (Ziggo-123Video).
Gerechtshof 's Gravenhage 15.11.2010, LJN BO3982 (Producenten geluidsdrager/St. de Thuiskopie).

Hoge Raad
Hoge Raad, 5.11.2005, C04/234HR, LJN: AU4019 (Lycos/Pessers).

Websites

Beck-aktuell Gesetzgebung, „Entwicklungsgeschichte",
<http://gesetzgebung.beck.de/node/1014619>.

J. Boie, „Geschäftsmodell Abmahnung", Süddeutsche Zeitung, 27. 2. 2010,
<http://www.suedeutsche.de/digital/illegale-downloads-geschaeftsmodell-abmahnung-1.8519>.

Bundesministerium der Justiz, "Besserer Schutz gegen überzogene Abmahnungen",
Nachrichten 3.11.2011,
<http://www.bmj.de/SharedDocs/Kurzmeldungen/DE/2011/20111103_Besserer_Schutz_gegen_ueberzogene_Abmahnungen.html>.

Bundesministerium der Justiz, "Entwurf eines Gesetzes gegen unseriöse Geschäftspraktiken",
Referentenentwurf 12.3.2012, <http://www.textintern.de/Bilder/Referentenentwurf.pdf>.

Deutsche Telekom, „Deutsche Telekom bietet anonymes Surfen mit IPv6", 23.11.2011
<http://www.telekom.com/medien/konzern/93240>.

Digiprotect, "FAQ – digiprotect", <http://www.digiprotect.org/html/faq.html>.

Eco – Verband der deutschen Internetwirtschaft e.V., „300.000 Adressen pro Monat: erfolgreicher Kampf gegen illegale Downloads“, Pressemeldung 31.5.2011, <http://www.eco.de/2011/pressemeldungen/300-000-adressen-pro-monat-erfolgreicher-kampf-gegen-illegale-downloads.html>.

ECP Platform voor de InformatieSamenleving, “Werkgroep Notice and Takedown”, <http://www.ecp-epn.nl/werkgroep-notice-and-takedown>.

Eerste Kamer, Auteursrechtbeleid, <http://www.eerstekamer.nl/kamerstukdossier/auteursrechtbeleid>.

Eerste Kamer, “Wet bewaarprlicht telecommunicatie”, <http://www.eerstekamer.nl/wetsvoorstel/31145_wet_bewaarplicht>.

M. Ermert, „Telekom verspricht IPv6 für Privatkunden-Anschlüsse bis Ende 2012“, Heise online 6.6.2012, <http://www.heise.de/newsticker/meldung/Telekom-verspricht-IPv6-fuer-Privatkunden-Anschluesse-bis-Ende-2012-1605061.html>

FBI National Press Releases, “Justice Department Charges Leaders of Megaupload with Widespread Online Copyright Infringement”, 19. January 2012, <http://www.fbi.gov/news/pressrel/press-releases/justice-department-charges-leaders-of-megaupload-with-widespread-online-copyright-infringement>.

Fraunhofer IIS, „The mp3 History“, <http://www.mp3-history.com/>.

Gulli – Der Unabhängige IT und Tech-Kanal! <www.gulli.com>.

Gulli, “Usenet“, <http://www.gulli.com/internet/filesharing/grundlagen/usenet>.

Gulli, “P2P”, <http://www.gulli.com/internet/filesharing/grundlagen/p2p>.

Gulli, “oneclickhoster”, <http://www.gulli.com/internet/filesharing/grundlagen/oneclickhoster>.

Heise online, „World IPv6 Launch Day: Das Experiment geht weiter“, 6.6.2012, <http://www.heise.de/newsticker/meldung/World-IPv6-Launch-Day-Das-Experiment-geht-weiter-1611755.html> / < http://heise.de/-1611755>.

Internet assigned number authority, <www.iana.org>.

Internet Society, “Gedragscode Notice and Take Down geode stap”, <http://isoc.nl/info/nieuws/2008-noticeandtakedown.htm>.

Dr. Noogie C. Kaufmann, , “’Geleakter’ Gesetzentwurf: Maßnahmen gegen Abmahnmissbrauch”, Heise online 17.4.2012, <http://www.heise.de/newsticker/meldung/Geleakter-Gesetzentwurf-Massnahmen-gegen-Abmahnmissbrauch-1540816.html> / < http://heise.de/-1540816>.

D. McCullagh, “FBI, DEA warn Ipv6 could shield criminals from police”, CNET 15.6.2012, <http://news.cnet.com/8301-1009_3-57453738-83/fbi-dea-warn-ipv6-could-shield-criminals-from-police/>.

Netzwelt, “IP-Speicherfristen: Wie lange speichern die Anbieter?“, <http://www.netzwelt.de/news/91086-ip-speicherfristen-lange-speichern-anbieter.html>.

Overheid.nl, <https://zoek.officielebekendmakingen.nl/dossier/29838>.

Platform voor Cybersecurity, <https://www.cpni.nl/informatieknooppunt/de-nationale-infrastructuur-ter-bestrijding-van-cybercrime-nicc>.

RIPE Network Coordination Centre, <www.ripe.net>.

RIPE Network Coordination Centre, “RIPE Database Query”, <https://apps.db.ripe.net/search/query.html>.

RIPE Network Coordination Centre, “IPv4 exhaustion”, <http://www.ripe.net/internet-coordination/ipv4-exhaustion>.

Stichting BREIN, “The BREIN Foundation”, <http://www.anti-piracy.nl/english.php>.

Stichting BREIN, “Ons Beleid”, <http://www.anti-piracy.nl/ons-beleid.php>.

Vereniging ISPConnect Nederland, “ISPConnect Notice & Takedown procedure”, <http://www.ispconnect.nl/ntd-procedure>.

Verein zur Hilfe und Unterstützung gegen den Abmahnwahn e.V., „Filesharing Abmahnwesen Deutschland Jahresstatistik 2011“, 10.2.2012., <http://www.verein-gegen-den-abmahnwahn.de/zentrale/download/statistiken/2011/jahresbilanz_2011.html>.

Wikipedia, “Binary file”, <http://en.wikipedia.org/wiki/Binary_file>.

World Ipv6 Launch, “Participants”, <http://www.worldipv6launch.org/participants/?q=2>.

Annex A: Short explanation of some Dutch and German terms:

Dutch terms:

Rechtbank	regional court
Gerechtshof/Hof	Higher regional court/court of appeal
Hoge Raad	Supreme court (highest court, no constitutional court)
Eerste kamer	Dutch council (upper house)
Tweede kamer	Dutch parliament / House of Representatives (lower house)
Laws:	
Auteurswet	Dutch Copyright Act
Burgerlijk Wetboek	Dutch Civil Code
Wet bescherming persoonsgegevens	Dutch Data Protection Act
other:	
reëel belang	a true/personal concern in something
"Art. [..] sub […]".	
"Art."	"Section" (Sect.)
"sub"	"paragraph"(para.)

German terms:

Amtsgericht	Local court
Landgericht	District court/regional court
Oberlandesgericht	Higher regional court
Bundesgerichtshof	Federal court of justice (supreme court in matters of criminal and private law)

Bundesverfassungsgericht	Federal constitutional court
Bundesrat	German federal council (upper house)
Bundestag	German federal parliament (lower house)

Laws:

Bürgerliches Gesetzbuch	German Civil Code
Gesetz über Urheberrecht und verwandte Schutzrechte	German copyright Act
Gerichtskostengesetz	Court Fees Act
Grundgesetz	German constitutional law/ Basic law
Strafprozeßordnung	German Code of Criminal Procedure
Teledienstedatenschutzgesetz	German Tele Services Data Protection Act
Telekommunikationsgesetz	German Telecommunication Act

Other:

Abmahnung	German cease and desist letter with the possibility to ask for reimbursement of expenses
Aktivlegitimation	right to sue
Richtervorbehalt	Requirement of judicial decree
Störer	secondary liable person

"§ (Paragraph) [..] Abs. (Absatz) [..] S. (Satz) […]" ; except Constitution, there articles are indicates as "Art. [..] GG".

"§"	"Section" (Sect.),
"Abs."	"paragraph" (para.), sometimes also translated as "subparagraph",
"S."	"sentence".
"Art."	"Section" (Sect.)

Annex B: § 101 UrhG

own non-official translation: *§ 101 Right to information*

(1) Whoever unlawfully infringes on a commercial scale copyright or other rights protected under this Act, may face a claim of the injured party of prompt disclosure of the origin and distribution of the infringing copies or other products. The commercial scale can arise both from the number of violations and the seriousness of the violation.
(2) In cases of obvious infringements or in cases where the injured party has brought action against the violator, the entitlement irrespective of paragraph 1 also against a person who on a commercial scale

1. had infringing copies in their possession,
2. was using infringing services,
3. provided services used for infringing activities or
4. was according to the statement of a in nr. 1, 2 or 3 named person involved in the production, manufacture or distribution of such copies, other products or services, unless the person would be under § § 383-385 of the Code of Civil Procedure be entitled to refuse to testify in a case against the violator. In the case of judicial enforcement of the claim pursuant the first sentence, the court may at request suspend the pending litigation against the offender until a final decision is reached in the litigation on the right to information. The party obliged to give information can claim from the injured party the necessary expenses for the provision of information.

(3) The party obliged to give information is required to give specifications of

1. Name and address of manufacturer, suppliers and other previous holders of copies or other products, the users of the services as well as industrial customers and retail outlets, for which they were intended, and
2. the quantities produced, delivered, received or ordered copies or other products as well as on the prices that were paid for the relevant copies or other products.

(4) The claims referred to in paragraphs 1 and 2 are excluded, if the claim is disproportionate in individual cases.
(5) If the party obliged to give information issues information which is intentionally or negligently false or incomplete, it is liable towards the injured party for compensation of any damage arising therefrom.
(6) Any person who has given a true information, without having been committed under paragraph 1 or 2 shall be liable to third parties only if he knew he was not obliged to provide information.
(7) In cases of obvious infringement, the obligation to provide information can be imposed by an injunction under § § 935-945 of the Code of Civil Procedure (“Zivilprozessordnung”).
(8) The findings may in criminal proceedings or in proceedings under the Administrative Offences Act for an offense against the obligated party or against a relative specified in § 52 paragraph 1 of the Code of Criminal Procedure (“Strafprozessordnung”) committed prior to granting the information not be used without the consent of the obligated party.
(9) If the information can only be given under usage of traffic data (§ 3 No. 30 of the Telecommunications Act), is for granting it a prior court decision required which sees upon the admissibility of the use of traffic data, and needs to be requested by the injured party. For issuing this order is solely responsible the district court (Landgericht) in whose district the party required to give information resides, has his seat or an office, without regard to the sum in dispute. The decision is made by the civil division. For the procedure, the provisions of the “Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit“ shall apply mutatis mutandis. The costs of the court order rest upon the requesting party. Against the decision of the District Court is appeal admissible. The appeal must be filed within a period of two weeks. The rules for the protection of personal data remain for the rest unaffected.
(10) By paragraph 2 in conjunction with paragraph 9, the basic right of telecommunications secrecy (Article 10 of the GG) shall be restricted.