(Johan Schlüter Law Firm - Office translation)

[Letterhead of the Copenhagen City Court]

ORDER

On 25th October 2006 in case No. FI-15124/2006:

IFPI Danmark
Højbro Plads 10
1200 Copenhagen K

acting for

Aller International A/S
Marielundsvej 46, E
2730 Herlev

ArtPeople
Ørstedhus
Vester Farimagsgade 41
1606 Copenhagen V

Bellevue Entertainment A/S
Slotspladsen 2
9000 Aalborg

Bonnier Amigo Music Denmark A/S
Gammel Mønt 14
1117 Copenhagen K

Circle Records
Bohelndachvej, Holmen
1437 Copenhagen K

Classico/Olufsen Records (single proprietor Peter Olufsen)
Uraniavej 12
1878 Frederiksberg C

COPE Records ApS
Westend 13
1661 Copenhagen V

Crunchy Frog ApS
Studiestræde 24, 2. sal
1455 Copenhagen K

Da Capo Records (independent institution)
Gråbrødre Torv
1410 Copenhagen K

Egmont Serieforlaget A/S

Vognmagergade 11
1148 Copenhagen K

EMI Music Denmark A/S
Dronningens Tværgade 7
1302 Copenhagen K

Exlibris Music Gyldendal A/S
Klareboderne 3
1001 Copenhagen K

Flex Records ApS
Magstræde 10B
1204 Copenhagen K

Folkeskolens Musiklærerforenings Forlag
Gudenåvej 162
7400 Herning

Forlaget GUF (single proprietor Jan Østergaard Nielsen)
Brogade 6
6400 Sønderborg

Hammock Music Group ApS
Vester Voldgade 87, 4. sal
1552 Copenhagen V

Intermusic (owner-managed business of Hans Jørgen Henriksen)
Øster Land 23
Sønder Ho
6720 Fanø

Kick Music A/S
Rådhusstræde 3A
1466 Copenhagen K

MBO Group A/S
Enghavevej 40, 4. sal
1674 Copenhagen K

MUSIC for DREAMS (owner-managed business of Kenneth Bager)
Magstræde 10
1204 Copenhagen K

Now Music I/S
Vognmagergade 7
1120 Copenhagen K

OH Music ApS
Jersie Strandvej 5
2680 Solrød Strand

Olga Musik ApS

Christianshavns Torv 2
1414 Copenhagen K

Playground Music Denmark A/S
Grønnegade 3
1107 Copenhagen K

RecArt Music ApS
Studsgade 10, 1. sal
8000 Århus C

Sand ApS
Lerholm Vænge 17
2610 Rødovre

SonyBMG A/S
Vognmagergade 7
1120 Copenhagen K

Spin.dk
Filmbyen 14
2650 Hvidovre

SteepleChase Productions ApS
Slotsalléen 16
2930 Klampenborg

Sundance ApS
Havnegade 41
1058 Copenhagen K

TUBA Entertainment (owner-managed business of Jerry Ritz Blom)
Søndre Jagtvej 27
2970 Hørsholm

Tutl (independent association)
Reynagøta 12
0100 Torshavn

Universal Music Group A/S
Grønningen 25, st.
1270 Copenhagen K

Warner Music Denmark A/S
Falkoner Allé 63
2000 Frederiksberg

Voices Music & Entertainment Denmark ApS
Vesterbrogade 95 H
1620 Copenhagen V

vs.

Tele2 A/S
Gammel Køge Landevej 55
2500 Valby

was made the following

ORDER:

During these enforcement proceedings, which were initiated on 13th July 2006, the Plaintiff, IFPI Danmark, acting for Aller International A/S, ArtPeople, Bellevue Entertainment A/S, Bonnier Amigo Music Denmark A/S, Circle Records, Classico/Olufsen Records, COPE Records ApS, Crunchy Frog ApS, Da Capo Records (independent institution), Egmont Serieforlaget A/S, EMI Music Denmark A/S, Exlibris Music Gyldendal A/S, Flex Records ApS, Folkeskolens Musiklærerforenings Forlag, Forlaget GUF (single proprietor Jan Østergaard Nielsen), Hammock Music Group ApS, Intermusic (owner-managed business of Hans Jørgen Henriksen), Kick Music A/S, MBO Group A/S, MUSIC for DREAMS (owner-managed business of Kenneth Bager), Now Music I/S, OH Music ApS, Olga Musik ApS, Playground Music Denmark A/S, RecArt Music ApS, Sand ApS, SonyBMG A/S, Spin.dk, SteepleChase Productions ApS, Sundance ApS, TUBA Entertainment (owner-managed business of Jerry Ritz Blom), Tutl (independent association), Universal Music Group A/S, Warner Music Denmark A/S, Voices Music & Entertainment Denmark ApS, has against the Defendant, Tele2 ApS, made the following claim:

1. That the Defendant be ordered not to aid to other persons' making available and making copies via the website, www.allofmp3.com, of sound recordings, to which the Plaintiff's members have the exclusive copyrights.

2. That the Defendant be ordered to make the necessary steps suitable for preventing the Defendant's customers to access the Internet website, allofmp3.com, and related sub-pages and sub-domains.

The Defendant has claimed that the petition for an injunction be denied.

The Defendant has also claimed that an injunction only be granted against a security of DKK 500,000.

Statement of claim and statement of defence

This case concerns the question, whether from the website www.allofmp3.com there is making available and making copies of sound recordings infringing the rights of Plaintiff's members under the Danish Copyright Act (Ophavsretsloven). The case also concerns the question, whether the transmission of the sound recordings in question, which takes place over Tele2' network, among other things, when Tele2's customers download the sound recordings in question via the telecommunication lines that Tele2 as Internet provider places at the disposal of its customers, represents an infringement of the copyrights of the Plaintiff's members.

The Plaintiff is the Danish branch of the International Federation of the Phonographic Industry (IFPI). The Plaintiff's members represent the vast majority of phonograms sales in Denmark.

Www.allofmp3.com is a Russian website, which is owned by the Russian firm Media Services, and which is offered on the Internet by the Russian Internet provider Real Time Network (ReTN).

On the website allofmp3 is published charts from a number of different countries, including the USA, the UK, Germany, and France. From the charts are links directly to the sound recordings sold on the website. Most of the music, which is offered on the Internet, is of foreign origin, but also a number of Danish artists are represented on the website.

From the website in question sound recordings are offered for download in compressed digital form, typically the mp3-format. The sound recordings are offered for download, according to the information given against payment of approx. USD 0.09-0.1 (approx. DKK 0.56 - 0.62) for a single sound track and approx. USD 1.09 (approx. DKK 6.75) for a whole album.

For comparison the Plaintiff has informed that the prices on Danish websites, which legally offer sound recordings for download, typically range from DKK 8.00 per sound track and DKK 96,00 for a whole album with 12 tracks.

The Plaintiff has furthermore informed that www.allofmp3.com in Great Britain has a market share of approx. 14% compared with other music websites.

For the purpose of this case, the Plaintiff has organised a questionnaire survey concerning the use of the website www.allofmp3.com in Denmark. The survey was undertaken by the advertising agency Just/Kidde A/S, which made the survey during the period of 6th - 16th June 2006. Among other things, the survey indicates that there was a market penetration for allofmp3 of minimum 2.10%. The conclusion runs:

> "Overall conclusion
>
> The survey has been made among 101 self-declared users of Allofmp3. Of these, around 50% are loyal users, as they have bought six times or more via the website.
>
> Nearly all buy foreign music, and about half of them buy Danish music. Single tracks are bought by 87%, while 74% buy whole albums. In general the website is used, because (in order of priority)
>
> - It is low-cost
> - The selection is large
> - It is easy to use.
>
> More than 1/3 are in doubt, whether Allofmp3 is a legal service, while 86% think that the service is legal.
>
> Around 2/3 also buy music from other sources. Around 20-25% acquires music by copying via the Internet, at the library or from friends.
>
> A large part of the respondents has Internet subscription with TDC (approx. 1/3), while Telia, Tele2, Cybercity and Sonofon also represent a substantial part by 5-10% each."

The parties are in agreement that under current Russian legislation it is illegal to make available sound recordings via the Internet without permission from the rightholder in question.

The Plaintiff has during this case informed that its members have not given permission to the making available and the copying that takes place via the website allofmp3. com.

It appears from the website allofmp3.com that the material made available via the Internet is covered by Russian licence # LS-3M-05-03 from Russian Multimedia and Internet Society (ROMS) and licence # 006/3M-05 from Rightholders Federation for Collective Copyright Management of Works used Interactively (FAIR). It is further stated on the website that Media Services pays a licence fee for all material downloaded from the website, in accordance with Russian law.

It appears from a declaration from the Russian branch of IFPI that neither the Russian section of ROMS, nor the Russian section of FAIR meets the criteria for being a collecting society under the Russian copyright act. It is further stated (in unauthorised translation):

> "More precisely, ROMS has not and has never had IFPI's members' permission to give allofmp3. com or any other similar website a licence to use the music recordings, which they own or to which they have exclusive licence rights, be it by reproducing, adapting, making available, offering for sale, selling or the like. IFPI's members have written specifically to ROMS to make it clear that ROMS has no right to give licence to the use of their music recordings.
>
> In addition, ROMS has not the necessary agreements with foreign collecting societies, nor does it distribute money to IFPI's members. On the contrary, as a result of its activities, including the allotment of a licence to Allofmp3, ROMS was on 21st October 2004 expelled from CISAC, which is the umbrella organisation of authors' collecting societies, due to its alleged unauthorised administration of rights. FAIR has never been a member of CISAC."

The Plaintiff has during these enforcement proceedings produced an opinion of 2nd August 2006, procured by the Plaintiff, from the IT-firm Contest A/S concerning the possibility to block access to a particular website. The statement contains, among other things, the following section:

> "The Anti-Piracy Group has addressed Contest A/S in order to have an expert opinion of the possibility of blocking access to a particular website, and how it is done in practical terms.
>
> As with the child pornography filter, which some genuine ISPs install to prevent their customers to gain access to this category of websites, one may block other sites and categories in a number of different ways.
>
> Method 1: Installation of hardware and software between the ISP's Internet connection and their customers' access

There are many different types of this kind of tools. In this opinion I will concentrate on one I know well, viz. Content Filtering from the American firm Sonicwall.

This is the solution we use ourselves in cooperation with the Danish National Library Authority (Biblioteksstyrelsen) and Atea in more and more libraries around Denmark to prevent the users in this country to access websites with pornographic contents.

In practical terms the solution consists of one or more units from Sonicwall with different capacity, but their common characteristic is that one can partly block access on the basis of a long number of categories such as pornography, hacker areas, areas with fanatical political messages, drugs and many other categories. Furthermore, it is possible to block areas on the basis of the website names and/or IP addresses.

The unit is placed as a filter between the ISP's customer area and their connection to the Internet. As mentioned, there are different varieties and sizes, but as the largest units can operate at a higher speed than most ISPs dispose of, this is not an argument for not acquiring them.

This solution is clearly the safest and the easiest for the ISP to use. It is therefore possible for the ISP to block the access to a particular website for all its customers, including the access to a website like www.allofmp3.com.

Method 2: Establishment of a so-called Proxy

It is possible for an ISP to ensure that all traffic to WEB (so-called http and HTTPS) is run through a so-called proxy server. This means that the users' machines are to be configured so that all traffic to WEB must takes place through a particular machine or machines with the ISP, so-called proxy servers. These proxy servers ensure the users' access to the Internet and can therefore be configured so that certain addresses are not allowed.

This is the solution, often in combination with method 1, that several large enterprises make use of, but as it requires powerful - and consequently expensive - equipment at the same time as the customers will be burdened with onerous configurations, this method is probably less interesting to ISPs.

Method 3: Blocking at DNS level

DNS (Domain Name Services) is the mechanism used to have web addresses translated to the unambiguous IP addresses, which the Internet operates with.

Many ISPs, including TDC, gives DNS access to their customers, and it will here be possible to stop translation of certain addresses to IP addresses, alternatively to pass on the inquiry to an address other than the address intended, and here give the user a warning that he is out on illegal business. However, this solution has the weakness that the user knowledgeable in IT may force another DNS server into his system other than the one that the provider offers and in this way gain access nonetheless to the unwanted sites.

Method 4: Blocking at IP level

In modern routers it is possible to put in filters that prevent access to particular sites, whatever it is done via IP addresses or via DNS references. The latter method will probably be rejected by the ISP, as DNS references may take time and thereby give disproportionate load on the router. It will be easier to block particular IP addresses, but it requires that the router is updated continuously, as the unwanted areas on the Internet in particular has a way of changing IP addresses from time to time, just as the same IP address may include both wanted and unwanted sites.

In principle, it will, however, be sufficient for the ISP to be given the name of a particular website - and thereby from that the IP address in question or a particular IP address and consequently block access to it.

I think that, in this connection, I owe to explain what a router is. A router is the unit that monitors the traffic from the ISP's network and thereby the ISP users to and from the Internet.

Information that an ISP needs to in order to block

If an ISP is to block a site, the only information it needs is the name of the site or the domain to be blocked. This also applies, if blocking is at IP level, as the ISP by so-called DNS references itself can gain access to the IP address applicable from time to time.

Conclusion

As appears from the above, there are consequently a large number of different possibilities available to an ISP to block access for its customers to a particular website. There are various advantages and drawbacks with the different methods, but they all give the possibility of efficiently blocking access to a given website.

…"

The Plaintiff has during this case declared that an injunction, if any, could be performed by the application of any of the four methods described above in the opinion. The Plaintiff will thus leave the choice of blocking method to Tele2.

It has been stated that the Plaintiff by letter of 5th May 2006 requested that the Defendant should avoid contributing to other persons' making available and copying of sound recordings from the website in question.

It has further been stated that the Defendant by letter of 26th May 2006 declined to comply with the request.

Witness statements

Erik Testman has explained that he is a self-employed businessman with his own IT firm. He has worked in the IT industry for 36 years. He has worked with network solutions since 1992, including for the Danish Prime Minister's Office (Statsministeriet) and other public institutions. For the last 10 years he has worked with network security. His company, Contest A/S, has itself operated as an Internet provider during the

period from 1997 to 2002, offering its customers' access to the Internet via the company's network. This part of the business operation was discontinued in 2002, because it was a poor business. However, the firm still has customers with mail access via the company's network. The firm has a co-operation with Atea and the Danish National Library Authority to avoid sites with pornographic contents. As for the four methods mentioned in the letter of 2nd August 2006, it is to be mentioned concerning method 1 that this is the solution used by the libraries. A unit reads all traffic on the network. Based on the patterns in the data traffic it can be seen, whether the contents are unwanted. The unit secures that vira do not enter and that no pornographic sites are shown. This equipment can also be installed at the Internet provider's with the purpose of avoiding websites with a particular content. It is sufficient that the unit knows the name of the actual website that one wants to avoid. It is not necessary to know the exact IP address. There are different organisations, which publish lists of websites with unwanted contents. He is familiar with the fact that Tele2 has a child pornography filter, but he does not know, which actual filer is used. A similar filter would be sufficient to prevent access to the website allofmp3.com. There are other filters with larger capacity than Sonicwall. Method 2, which involves that the machine is connected to a proxy server, is not used so much any more. There is copying and intermediate storage of actual websites every time a user has visited a particular website. The means that the copy of the website exists on the proxy server for a certain period of time. The proxy server can be configured so it does not accept particular websites. Method 3 exploits the fact that inquiry must be made to a DNS server to have converted the name of the website to an IP address. The Internet provider can, however, block references on the DNS server for particular websites, so that the Internet user in question is instead directed to another site with a warning against the particular website or to a "dummy" site, or that the inquiry just does not result in a reply. This solution will work with the ordinary, average user, but not for the technically knowledgeable user who will be able to circumvent the block by configuring his pc so it addresses the inquiry to the DNS server via a proxy server. The pc's configuration can be changed by a very few clicks, if one knows how to do it. If a guide is written, most ordinary users would also be able to find out how to change their pc's configuration. It is theoretically possible that the user may circumvent the block of the DNS server by writing the actual IP address instead of the website's name, but it is not certain that a connection to the website will be established. The matter is so that there is a shortage of IP addresses. This has lead to the situation that more Internet providers' customers have to share the same IP address. When the web server receives an inquiry, it directs the inquiry to the right website by the help of the name of the website. If only the IP address is indicated, the web server does not know, to which website a connection is wanted. Many enterprises have their own DNS server, which has been configured to communicate with the Internet provider. The enterprise may consequently decide which websites their employees may have access to. A block via DNS server will also affect enterprises with their own DNS server. Method 4 entails that the router is configured so that the user is not offered access to certain IP addresses. It is a facility that is possible with modern router equipment. The user will not at all discover what happens. To the user it will appear that nothing happens. It will not help that allofmp3.com possibly changes its IP address, as this sooner or later will be updated in the DNS server, whereby the block continues to be in force. Method 4 is the most onerous and the most expensive solution. Method 3 is the simplest and most cost-effective solution. Theoretically a filter could be applied to DIX, which is the connection and exchange central of data traffic between Internet providers in Denmark, and through which most of all data traffic out of Denmark passes. In practice, however, it cannot be done, as there is too much traffic through DIX. As he does not know Tele2's network, he cannot answer, whether it is necessary to set up filtering equipment on all the 125 telephone ex-

changes in this country, on which Tele2 has rented capacity. Data files that are sent via the Internet are divided into packets of maximum 1.500 bytes. A file of 5 megabytes will thus be divided into 3,000 packets. Each packet is sent off, often via different networks, to be assembled again at the receiver. He cannot answer, for how long such a packet will be in the router. If the sender does not receive notice that the packet has been received at the place of destination, the packet will be sent off again, or it will be lost. There is a technical intermediate storage of the package in the router. It takes a millisecond. The signal, which has been sent through the router, is logged, among other things, with the purpose of charging a fee.

Thomas Lehmann has explained that companies may establish their own DNS. The most common thing to do is to use the provider's DNS, as it results in the fewest problems.

Henrik Bo Hansen has explained that he has been employed at Tele2 for 10 years, the last two years as net operation manager. He is familiar with the decision that the Danish Supreme Court delivered on 10th February 2006 in the case between TDC and the Plaintiff. There are certain differences in terms of infrastructure between Tele2 and TDC. He is consequently familiar with the fact that TDC has previously used proxy servers a lot. On these proxy servers TDC has stored data in order to make them available quickly to the users. In the decision of February 2006 the user of the website was a customer on TDC's own net. When TDC closed down the website, it became unavailable to all, also to persons who were not customers with TDC. If Tele2 closes allofmp3.com, it will only have significance for Tele2's customers. All other Internet providers will still allow access to allofmp3.com. The proposals, which Erik Testmann have presented, are a solution, which would be typical of a smaller, Danish enterprise. Method 1 is not possible to use today, at least not without extraordinary costs. It would require a purchase of equipment at DKK 5-10 million. The method would demand that filters had to be installed on many of the exchanges, where Tele2 has set up its own equipment. For some exchanges, more boxes would have to be installed. To improve the traffic through the Internet for Tele2's customers, one would all the time have to attempt to create redundancy, i.e. that there has to be as many routes as possible, through which the traffic can be sent. Consequently, there are many places where to install a box. There are boxes with can make "content filtering". If the user knows how, he can, however, circumvent "content filtering". To this is added that these boxes often do not allow data transmission via the HTTPS protocol, i.e. that the user cannot obtain access to a pc bank or similar services that uses this protocol. Method 4 is practically feasible. The method requires that the configuration is changed centrally by inserting an IP filter. The router will then examine all packages sent through it. If the router cannot handle the packet, it is discarded. That can give transmission problems in the system. This method could, furthermore, also be circumvented. Method 2 requires a proxy server to be set up on all exchanges, or alternatively that a proxy server is connected centrally. The latter solution will, however, have the effect that redundancy is counteracted. The method has the unfortunate consequence that there is no access to payment sites on the Internet. Method 3 intervenes in the name server hierarchy on the Internet. In principle a zone, which is called allof, can be established, and then it will be possible to determine, what people may see, when this name is referenced. Technically this is an incorrect solution as one may therefore end in the situation where two persons, who each have their own Internet provider, by referencing the name allof may come to different results. In principle it should be so that one reference gives the same result no matter which provider one uses. Method 3 is easy to circumvent just by changing the computers configuration. The method can also be circumvented by using the IP address instead of the name. To this is added that not all

Tele2's customers use Tele2's DNS. There is no copying of files in the router. There is no logging mechanism in the router. If the router cannot send the file, it will be dropped. There is then message to the sender that the file has not been received. The file will then be sent again. At no point in time are there two copies of the file, i.e. an original and a copy. The file will be copied only purely technically in connection with the forwarding through the network. The file remains in the router for less than a millisecond. The mp3 files are never present in the router. If the file goes through a proxy server, there will in all probability be a copy of the mp3 file on the proxy server. Registered.com is the authoritative name server to allof, i.e. that it has the rights to monitor allof on the Internet. If the injunction instead was directed against Registered.com, it would be avoided that the injunction could be circumvented by a changed configuration as concerns the name server. Registed.com is situated in the USA. Allofmp3.com would not be able to notice it, even if all traffic from Denmark is stopped. If one imagined that traffic to allofmp3.com from all Europe was closed down, Media Services would probably develop a programme that would allow its customers to get in touch with them anyway. If one, say, referenced music.allof, one would reach allofmp3.com's website. If an enterprise has its own DNS, it would not reference via Tele2's DNS, but in accordance with the protocol laid down for the enterprise. Tele2 filters on the domains classified as child pornography. There is a register of such domains kept and administered by the Danish Commissioner of Police (Rigspolitichefen). Tele2 has no administration in connection with this filtering, as it is the police who decide which domains are entered into the register. Filtering for child pornography is done at DNS level.

Closing oral submissions

The Plaintiff has claimed

that from the website, www.allofmp3.com, is made available sound recordings, to which the Plaintiff's members have the exclusive copyrights;

that the sound recordings are made available, so the users may download (copy) these against payment;

that this making available of the sound recordings constitutes a separate public performance, cf. Section 2 (3) No. 3 of the Danish Copyright Act;

that nor have the Plaintiff's members or their foreign sister companies made agreements of any kind with the Russian organisations, ROMS and FAIR;

that ROMS and FAIR are furthermore not legitimate collecting societies;

that this making available consequently is an infringement of the exclusive copyrights of the Plaintiff's members;

that the contents of www.allofmp3.com are infringing;

that even the charts, which are available on the website, consequently are infringing, as the charts contain links to the sound recordings, which are sold on the website, and as linking to copyright-protected material on websites represent a making available to the general public, cf. e.g. the Danish weekly law report UfR 2001.1572V;

that the Defendant has not otherwise documented that the users of www.allofmp3.com use the website for legitimate purposes;

that in any event, an injunction may be issued against a website, from which are made infringements of copyright-protected material, even though the individual user just browses the websites in question, but do not make copyright infringements, cf. the Danish weekly law reports UfR 2001.1572V and 2005.60V;

that the users' purchase and thereby download of digital copies of sound recordings, which are made available via the website, www.allofmp3.com, represent an illegal copying, cf. Section 2 of the Danish Copyright Act, cf. Section 11 (3), cf. Section 66, (1) and (2);

that it is established that among the Defendant's customer is a substantial number of users of www.allofmp3.com;

that the Defendant's customers buy and download digital copies of the sound recordings that are made available via the website;

that the Defendant aids to the illegal copying and making available by transmitting the sound recordings made available illegally;

that it has been documented that by transfer of data in a network there is a technical copying of such data;

that the Danish Supreme Court by its decision of 10th February 2006 has held that copying takes place by transmission in a tele company's network;

that this temporary copying is infringing, cf. the Supreme Court decision of 10th February 2006 in case No. 49/2005;

that the Defendant's customers can only access the website via an Internet subscription with the Defendant;

that the Defendant consequently is a necessary connecting link in the illegal transmission;

that there consequently is made copies of infringing material in the sense of the Copyright Act and the E-Commerce Act by the Defendant's transmission of data from www.allofmp3.com to the Defendant's customers;

that the exemption of Section 11a of the Copyright Act does not apply to this transmission, as Section 11a of the Copyright Act presumes that the copies are made from a source, cf. Section 11 (3) of the Copyright Act;

that the Plaintiffs do not claim damages or criminal liability against the Defendant, as he is exempt for liability, cf. Section 14 of the E-Commerce Act;

that it follows from the explanatory notes to the Danish E-Commerce Act that the provisions on liability exemption in this act do not include interim remedies, including injunctions;

that Section 14 of the E-Commerce Act does consequently not exclude that an injunction may be issued against the Defendant's acts that infringe the exclusive copyrights of the Plaintiff's members;

that the Defendant transmits infringing contents from www.allofmp3.com to its customers through the Defendant's network;

that the Plaintiffs have a substantial, protectable interest in putting a quick and efficient stop to the infringements that take place via www.allofmp3.com;

that a block of the transmission of the infringements made by the Defendant is the quickest and most efficient method to safeguard this interest;

that in accordance with case law exemplified by the Supreme Court order of 10th February 2006 in case No. 49/2005, an injunction can be issued against the Defendant;

that it appears from Article 8 (3) of the Infosoc Directive and its preamble and from Supreme Court case law that the right to have issued an injunction against a tele company exists notwithstanding the possibility of prosecution of infringements elsewhere;

that a requirement that the Plaintiffs should attempt to have the infringements stopped elsewhere, e.g. in Russia, would consequently not be in accordance with Supreme Court case law and the Infosoc Directive;

that such a requirement would furthermore mean that the infringements made on www.allofmp3.com could not be stopped in practice;

that such a requirement would furthermore be in contravention of the legislative history of the Copyright Act, Community law and Supreme Court case law;

that such a result would be disproportionate and disregard the Plaintiff's interests in having the infringements stopped;

that the Plaintiffs are prepared to let the Defendant's duty to act be restricted to include blocking at DNS or name server level.

In support of the fact that the Danish Administration of Justice Acts conditions for issuing an injunction have been met, it is submitted

that the legislative history to the provisions on injunctions and case law allow that opinions obtained by one party are submitted in enforcement proceedings;

that the Defendant has also produced opinions obtained by himself, why the Plaintiffs are of the opinion that the Defendant has waived his submission of this item;

that the actions sought to be restrained are clearly infringing the copyrights of the Plaintiff's members:

that the illegal activities sought to be restrained is to be expected to be continued:

that the general rules of Danish law on penalties and damages do not give the Plaintiffs adequate legal protection, as it is noted that legislator in connection with the tightening of the conditions in the Administration of Justice Act for issuing injunctions, has expressly stated in the preparatory works that the conditions for an injunction will generally have been met in cases of infringements of intellectual property rights, cf. Section 642 of the explanatory notes to Section 642 of the bill;

that an injunction as requested by - and as restricted technically as described - the Plaintiffs do not exceed the duty to act that the Defendant may thereby be imposed;

that the Defendant can technically comply with such an injunction;

that theoretical, technical circumvention possibilities do not exempt the Defendant from his obligation to stop the illegal activities;

that the Plaintiffs have a significant and protectable interest in having stopped the illegal transmission, which exceeds the Defendant's interest in continuing the illegal activities;

that an injunction thus is proportionate, cf. Section 643 (2) of the Danish Administration of Justice Act.

In connection with the execution of the injunction it is claimed

that the Defendant's customers, which are prevented access to the website, www.allofmp3.com, would not be able to direct a claim for damages against the Defendant, as the customers themselves act in contravention of the exclusive copyrights of the Plaintiffs' members pursuant to the Copyright Act, if they download sound recordings from the website;

that the Defendant consequently cannot incur any loss by the issuing of the injunction;

that this is in accordance with case law; cf. the decisions of the Supreme Court and the Eastern High Court;

that the Plaintiffs consequently are not to provide security in connection with the execution of the restraining order.

The Defendant has claimed:

that the motion for injunction be refused, as the conditions stipulated in Section 641 of the Administration of Justice Act have not been met, as it is claimed in particular

that it has not been proven or rendered probably the acts that the Plaintiff wish to be restrained are unlawful, as it is claimed in particular

that it has not been documented that www.allofmp3.com infringes the Plaintiff's rights;

that it has not been documented that www.allofmp3.com in its entirety infringes the Plaintiff's rights;

that the Defendant has not had any knowledge of the infringements;

that there is not made copies of works from www.allofmp3.com, which is covered by the Copyright Act, in the Defendant's networks;

that the injunction required is disproportionate, cf. Sections 642, No. 3, and 643, as it is claimed in particular

that the proportionate legal action would be to initiate legal actions directly against www.allofmp3.com;

that other more proportionate legal actions would be to bring legal action against retn.ru, which is the provider that www.allofmp3.com uses, or the American company register.com, which administers the name server of www.allofmp3.com;

that there are no exceptional difficulties in connection with countering www.allofmp3.com in Russia with adequate legal measures, if www.allofmp3.com, as claimed by the Plaintiff, is illegal and infringes the Plaintiff's rights;

that it will be possible, in particular after the amendment of the Russian copyright act on 1st September 2006, to counter the claimed infringement by www.allofmp3.com in Russia;

that the reason for the Plaintiff to request an injunction against the Defendant is that he does not want, for reasons of lack of resources, to pursue www.allofmp3.com directly;

that it is not technically possible to carry out the restraining injunction;

that users of the Defendant's network without difficulty may circumvent possible technical implementations of the restraining injunction;

that it has not been documented that there are Danish users of www.allofmp3.com, including users who use the Defendant's network;

that the Plaintiff has exercised passivity in the pursuance of his claim for the issuing of an injunction, as it is claimed in particular,

that injunctions may only be issued, if the Plaintiff pursues his claim without unreasonable delay;

that the Plaintiff has known of www.allofmp3.com for at least two years;

that awaiting the Supreme Court's decision of 10th February 2006 does not suspend passivity;

that the Plaintiff since the Supreme Court order on 10th February 2006 has exercised passivity by not submitting the request for injunction until 11th July 2006;

that the Plaintiff is to provide security for the injunction, if decided, with at least DKK 500,000 to secure any claims from customers against the Defendant in connection with the blocking of access to www.allofmp3.com;

that it is to be prejudicial to the Plaintiff's case that the Defendant's requests for information have not been met, and

that the expert opinions submitted by the Plaintiff have been obtained by him and therefore they have only limited value as evidence.

The Court's reasons and decision

Based on the evidence given the Court is satisfied/ finds it has been rendered probable that the Russian firm Media Services, which offers the website www.allofmp3.com, does not have the necessary permission from the Plaintiff, who administers copyrights to phonograms in Denmark, to make, via the Internet, protected works available to the general public. The Court has in this connection in particular had taken into consideration the very low price, at which the music works are offered on the website, just as the Court has had regard to the information from the Russian section of IFPI, according to which the Russian section of ROMS does not have the permission of IFPI's members to give Allofmp3 or any other similar website a licence to use the music recordings, which they own and to which they hold the exclusive rights.

It remains uncertain, to which extent the Russian website has Danish users who download protected music works. The questionnaire survey produced by the Plaintiff and prepared by the advertising agency Just/Kidde A/S indicates a market penetration of minimum 2,10%. Even though the survey is to be read with some reservations, partly because it has not been carried out on the basis of a representative section of the population, but is only based on answers from respondents who have bought music from allofmp3.com within the last year, and because the number of respondents is very limited, it seems, however, to render probable that the use of the website has a certain extension in Denmark. In favour of this argument is the fact that the website was included in the Danish consumer magazine "Tænk"'s survey from April 2006 of the market for download of music. Finally - and most conclusively - the fact that allofmp3.com offers sound recordings of Danish artists for sale, pleads with considerable weight for the website also being directed at the Danish market. As a result of the market share that Tele2 has as a network operator, it must be assumed that a proportional share of Tele2's customers download music files from the website in question. The transmission of the music files take place in these instances through Tele2' network.

Tele2 has indicated that the temporary intermediate storage, which takes place in the router - when the music files are sent via the Internet - and which is carried out in less than a millisecond, is so short-lived that it is not a matter of making copies as mentioned in Section 2 of the Copyright Act. Tele2 has in this connection underlined that TDC - at least previously - has used proxy servers to a large extent, and that the decision reported in U2006.1474H must be judged on this background, as copies undoubtedly are made in proxy servers. Tele2 does not use proxy servers, however.

Pursuant to Section 2(2) of the Copyright Act, making of copies is considered to be any direct or indirect, temporary or permanent, in whole or in part, copying in any way

and form whatsoever. Any form of copying is consequently covered by Section 2. The Court finds on this basis that also the short-lived and random fixation of the music work in the form of electronic signals, which is made in the various routers during the data packet's transmission via the Internet, is covered by Section 2 of the Copyright Act. Tele2 may not, furthermore, invoke the right to make temporary copies pursuant to Section 11a, as this provision presumes that the copies are made from a lawful source.

In accordance with the decision reported in U2006.1474H, Tele2's transmission of the works causes Tele2 to infringe objectively the copyrights administered by the Plaintiff, cf. Section 2 (2) of the Copyright Act, cf. Section 2 (1).

It is not rendered probable that allofmp3.com is also used for legal purposes, despite the fact that it is formally possible for the users only to make themselves familiar with various charts without downloading music. The structure of the charts with direct links to the music files in question, which then may be downloaded, may on the contrary be considered an integral part of the concept applied.

It must also be considered that the infringing activities will continue, unless an injunction is issued. The conditions stipulated in Section 642 of the Administration of Justice Act are thus to be considered to have been met.

The Plaintiff has produced information on various methods, by which the injunction, if issued, could be complied with, and has left it to Tele2 to decide itself, which of the methods described should be used if necessary in order to comply with the injunction. The method that consists of blocking at DNS level corresponds to a wide extent to the method used today by most Internet providers to block child pornography. It has thus not been rendered probable that it is technically impossible to effect an injunction. Blocking at DNS level may furthermore be assumed to be carried out without any noticeable costs or administrative effort to Tele2. The circumstance that a blocking might be circumvented by more experienced IT users, as is also the case of blocking of child pornography, is not found in itself to prevent that the injunction is complied with.

It cannot be refused that it might be possible through legal proceedings or other legal actions directly against Media Services or the Internet provider in Russia to take measures against the website in question. When considering the principle of proportionality the Court attaches, however, importance to the fact that a request that all remedies be first been attempted in Russia, would mean that the illegal activity could continue for yet some time with the result of losses to the Plaintiff. It would furthermore be in contravention of Denmark's obligations under Section 8 of the Infosoc Directive, which was implemented in Danish legislation by act No. 1051 of 17th December 2002 on the amendment of the Copyright Act, according to which rightholders are entitled to request an injunction issued against intermediaries, whose services are used by third parties to infringe copyrights or related rights. The reason, among others, for these provisions is that such intermediaries are in many cases the best persons capable of stopping the infringements.

From information presented in this case it appears furthermore that the Plaintiff in late 2005 began securing evidence with a view possibly to file a motion for an injunction. It has further been informed that the Plaintiff then decided to await the decision reported in U2006.1474H, and that the Plaintiff in the spring of 2006 made additional securing of evidence, before he in early May 2006 addressed Tele2 with a request that

the Defendant should avoid contributing to the making available and copying sound recordings from the website in question, which was declined by Tele2 on 26th May 2006, after which the motion for an injunction was filed on 11th July 2006. It is also noted that, based on the evidence, it must be taken into consideration that the number of Danish music works offered for sale via allofmp3.com has increased during the period from late 2005 to spring 2006. Under these circumstances the Court does not find that the Plaintiff has exercised passivity in respect of petitioning an injunction against allofmp3.com.

There is no basis to assume that the Defendant would incur liability for damages, neither from its subscribers, nor from any third party, by complying with the injunction. For that reason there is no reason to make a claim for provision of security.

The Enforcement Court consequently allows the Plaintiff's claim as ordered below.

It is held:

The Defendant, Tele2, be ordered to discontinue to aid to other persons' making available and making of copies via the website www.allofmp3.com of sound recordings, to which the Plaintiff's members have the exclusive copyrights.

The Defendant is further ordered to take the necessary steps suitable to prevent the access of the Defendant's customers to the Internet website, allofmp3.com and related sub-pages and sub-domains.

[signature]
Marianne Lund Larsen
Judge

[stamp 25th October 2006]

[stamp:
This is to certify the authenticity of the transcript
25th October 2006
Enforcement Court of the Copenhagen City Court]

[signature]
Ulla M. Larsen