

How to Solve Copyright Problems in P2P Content Distribution?

Ville Oksanen, Mikko Välimäki and Olli Pitkänen

[ville.oksanen, olli.pitkanen]@hiit.fi

Helsinki Institute for Information Technology

mikko.valimaki@hut.fi

Software Business and Engineering Institute

P.O.Box 5400, FIN-02015 HUT, Finland

Tel: +358 50 598 0498; Fax: +358 9 4513293

Abstract. This article discusses the copyright problems in peer-to-peer (P2P) content distribution systems. The article starts with a short survey of P2P technologies, their current use and legal problems so far. We argue that different copyright problems can be addressed either with digital rights management (DRM) and licensing technologies or a levy system in copyright law. Although DRM has been pushed strongly forward by the industry, we take a critical look at its possibilities in P2P.

Keywords: Copyright, Peer-to-Peer (P2P), Digital Rights Management (DRM)

1 Introduction

The term *paradigm change* describes very well what is happening currently in the content industries. The Internet has not treated the owners of copyrighted works well. The level of unauthorized copying has been staggering since the invention of the present-day P2P networks. The offered solution, DRM, has yet to prove its soundness. The digital dilemma has still to find its answer. (Digital Dilemma 2000).

In this article we first take a hard look into current situation pertaining both P2P networks and DRM. With P2P, we refer generally to communications that travel from one user's computer to another user's computer without being stored on a central server. With DRM, we refer to a set of legal and technical tools for managing rights in information products (Pitkänen and Välimäki, 2000).

In the second part of the article we analyze what kind of copyright issues must be taken into account while improving these systems. The analysis is mostly based on court cases on copyright law although we understand there may be more specific copyright problems stemming from specific technical and business issues. For instance, a business objective of different pricing and payment methods for content poses legal requirements for handling the licensing of copyright accordingly.

Obviously, from numerous court cases we can see that P2P developers should pay more attention in “legal requirements engineering”. We argue that copyright requirements can be incorporated into P2P systems e.g. with digital rights management (DRM) technologies or by implementing a levy system in copyright law.

2 P2P and Legal Problems So Far

2.1 Classification of Peer-to-Peer Systems

P2P systems are now gradually replacing client/server -based systems as the users’ primary method for searching and managing certain types of digital information. During the last five years, P2P services have become more effective, widely available, more usable, and have reached a critical mass.

For the purpose of this article a relevant way to classify P2P systems is the following:

| <i>Centralized</i> | <i>Hierarchical</i> | <i>Decentralized</i> |
|--------------------|---------------------|----------------------|
| (Original) Napster | Usenet | Gnutella(2) |
| Aimster | IRC | Fast Tract [KaZaA] |
| Audiogalaxy | DirectConnect | Ares |
| MyNapster | EDonkey2000 | Freenet |

Table 1. Classification of P2P systems (Hong).

In this classification we have first centralized P2P systems. A centralized system is coordinated and controlled by a central server. Only the data is distributed across of users’ hard disks. Music sharing applications Napster, Audiogalaxy and Aimster used to be good examples of this type of programs but now they are all sued into oblivion.

Second, we have hierarchical systems. There might have coordinators in different levels of the hierarchy each having local autonomy over its domain. Usenet is a proper example here.¹ IRC is another classic example fitting into this category. More modern hierarchical P2P approach can be found from e.g. DirectConnect. Edonkey2000 uses servers but increasingly supports also fully decentralized network.

Third, decentralized systems have no global coordination. Hence, the system architecture limits the possibilities to control the system from inside. Ares, Gnutella(2), Freenet and Fast Track are describing examples.

Many modern P2P clients offer access to multiple networks. Examples of this are Shareaza, which supports BitTorrent, eDonkey and Gnutella2; and Sigster, which support BitTorrent, eDonkey2k and FastTrack.

Table 2 offers a more detailed view to the features of some of the most popular P2P-services to date. It classifies the services with nine different attributes:

| Program | Napster | Usenet | DirectConnect | EDonkey2000 | KaZaA | Ares | Freenet |
|--------------------------|-------------------------|---------------------------|-------------------------|------------------------------|----------------------------|-------------|----------------|
| Basic Architecture | Centralized | Hierarchical | Hierarchical | Hierarchical/ Distributed | Distributed | Distributed | Distribu |
| Protocol | Proprietary (hacked) | Open Source | Proprietary (hacked) | Open Source | Proprietary (hacked) | Proprietary | Open Source |
| Search method | Centralized | Centralized | Centralized | Hierarchical/ Distributed | Distributed +supernodes | Distributed | Distribu |
| Data storage | Distributed | Distributed at servers | Distributed | Distributed | Distributed | Distributed | Distribu |
| Have to share | No | No | Typically yes | No | No | No | Yes |
| Anonymous uploading | No | No | No | No | No | No | Yes |
| Anonymous downloading | No | No | No | No | No | No | Yes |

Table 2. Some features of P2P systems that have been popular.

2.2 Legal problems of centralized systems

¹ Although since Usenet relies on centralized servers in the information distribution, one may argue whether Usenet is a P2P service at all.

To date, the most successful legal cases against P2P systems have been targeted at start-up companies that offer client software for centralized systems. Napster was the first victim to fall after highly visible court battle in California. (RIAA 2003b) Similarly RIAA managed to force Aimster and out of business by acquiring injunction (RIAA 2003a) and made a settlement with Audiogalaxy, which forced it to close its P2P-network (Menta 2002).

The reasons for choosing the centralized systems as the first target for lawsuits was evident. First centralized systems have one point, which can be attacked at, and perhaps has even wealth or visibility. One could argue a centralized system by definition has legally a *weak point* (Välimäki and Martikainen 2000). The owner of the central server has possibility to control the whole P2P network and thus he has responsibilities. It is much harder to find someone to sue in a decentralized system and even if a single user is identified and prosecuted successfully, it does not kill the system as a whole. The second reason is that centralized systems used to be the most successful in terms of users and transferred files (Harmon 2000).

Up to now, the most important court cases have been in the US. The detailed legal reasoning has been based on tertiary contributory copyright infringement. Three elements are required to establish the contributory liability of a party for copyright infringement. The first and most obvious requirement is that there is infringing activity. The other requirements are that the owner of the service must have knowledge of the infringing activity and somehow contribute to the infringing conduct. In the Napster case it was quite clear from the beginning that all of these requirements were met, even though the legal team of Napster made its best effort to blur the facts (A&M Records v. Napster 2001).

2.3 Legal problems of hierarchical systems

The first copyright case aimed at a hierarchical P2P service provider was RTC v. Netcom, again in the US. In this case the church of scientology (RTC) sued the ISP (Netcom) for infringing material posted by a third party on a Netcom's Usenet server. Netcom refused to exclude the third party's access to the Usenet unless RTC proved that they owned the copyrights to the material at issue. The court decided that Netcom was not liable, but the reasoning behind the decision left many questions open. (Raquillet 1999)

This legal uncertainty was one step on the way of the US Congress to add *safe harbour* provisions to the Digital Millennium Copyright Act (DMCA). The intention of the provisions is to exempt liability for merely providing communication facilities. These provisions give protection to eligible service providers by limiting the remedies that can be sought against the (DMCA Sec. 512). A similar safe harbour provision can be also found in the EU's Electronic commerce directive (Electronic Commerce Directive 2000). For convenience, we refer in the following to DMCA provisions.

The definition of a service provider in the DMCA is very broad: “a provider of online services or network access, or the operator of facilities therefore.” (DMCA Sec 512 (k)) This definition has been tried to use to protect a P2P application first in the Napster case. Unfortunately, Napster didn’t fit in because it is a centralized service. However, it is arguable that the definition should be broad enough to include at least some hierarchical P2P services.

In the case a P2P system qualifies as a service provider, it is relatively easy to take advantage of the safe harbour provisions. In the US, a service provider must further pay a fee and comply with certain requirements for reporting and other activities. Moreover, the service provider must adopt and implement a policy for the termination of repeat infringers and must appoint an agent to receive notifications of claimed infringements. (DMCA Sec 512 (c))

The service provider is not allowed to interfere with “standard” technical and legal measures used by copyright owners to identify or protect copyrighted works. What does this mean is still unclear, but it might include standard DRM measures like digital watermarks or copy protection schemes. (DMCA Sec 512 (i) (2))

Lastly, it is noteworthy that the copyright owner can - regardless these safe harbour provisions - sue the direct infringer, which can be virtually any user or participant in a hierarchical P2P system. This is not only theoretical speculation, but it has happened earlier in practice. For example Scientology started suing individuals after its case against Netcom failed (Newman 1996) and FBI raided users who were very active participants in Direct Connect -network (Ashcroft 2004).

2.4 Legal problems of distributed systems

Distributed P2P systems have been so far the most resistant to legal measures - maybe because there hasn’t been in many cases any company backing up the system or benefiting from its use that could have been sued. Instead, the users of such systems have been targeted extensively by the copyright holders.

The users who are sharing their files are in most cases violating the copyright holder’s right to distribute the work in public. This means that if these persons can be identified,

they can be sued effectively. Only if file sharing is limited to a small and closed circle of people (friends), it is possibly considered as private use.²

RIAA in the United States has been pushing the court case strategy against individual users very aggressively. It has sued so far thousands of P2P users in the United States. The similar process is also starting in Europe, although there have already been some scattered cases at least in Finland and Denmark. The right holders cannot naturally sue all the millions of users but instead they aim to rise the risk of using P2P systems so high that the payoff is not longer positive compared to acquiring the music from legal sources.

The technologies itself are most likely legal at least under current copyright legislation. In 2002, Kazaa was found to be legal in the Netherlands. Also in a more recent Grokster case in the United States the court found the company behind Grokster not liable for the copyright infringement done by the users. The case gave also some further guidance about the limits of liability:

- The Court stressed that in the “Betamax defense” the important question is whether a technology is merely capable of a substantial non-infringing use, not the proportion of non-infringing to infringing uses. The entertainment industry has suggested the opposite, which would have offered an easy way to kill off new technologies.
- The Court state that the Betamax defense is valid as long as the copyright owner can not show that the technology developer had (1) knowledge of specific infringements (2) at a time when it could do something about those infringements.
- The Court made it clear that copyright law does not require technology developers to design only the technologies that the entertainment industry would approve.
- The Court observed that, in the long run, a competitive, unfettered market for innovation ends up helping copyright (Von Lohman 2004a).

Because of the failures in court, the copyright industry is currently pushing for legal changes, which would outlaw the distributed file sharing technologies. For example, they have lobbied extensively for so called “Induce -act”, which would make a small but very substantial change to the copyright act:

“(g)(1) In this subsection, the term ‘intentionally induces’ means intentionally aids, abets, induces, or procures, and intent may be shown by acts from which a

² Although this can be seen as acting against the intention of the copyright law.

reasonable person would find intent to induce infringement based upon all relevant information about such acts then reasonably available to the actor, including whether the activity relies on infringement for its commercial viability.

“(2) Whoever intentionally induces any violation identified in subsection (a) shall be liable as an infringer..” (Induce Act 2004).

2.5 Other technologies

Some of the more advanced distributed P2P systems use so called *swarm-technology* for file-storage. In this method, a single user is hosting only small parts of the files. So far these systems have not been very successful. Mojo Nation, which has been lately in a dormant state, describes their system in the following way:

“Content stored using the Mojo Nation technology is formatted as hundreds or thousands of small, replicated fragments of the original data source. When a peer downloads data using our content distribution technology the local client pulls the file fragments in parallel from its peers; like a swarm of ants cutting up and transporting food to the nest, a retrieval in Mojo Nation is able to harness dial-up and other low-bandwidth users together into a team to deliver rich-media and streaming content.”

From legal perspective, this model makes it very hard to pinpoint a single source of the infringement and offers therefore perhaps a practical way to avoid liability. On the other hand, it is also possible to argue that all the users who form the swarm are equally liable for the infringement.

3 DRM and Its Application Sphere So Far

3.1 A Short History of DRM

The idea behind digital rights management is not a new one although the term DRM has been in general use only for a couple of years. Few large companies and public entities started research in “electronic copyright management” in the 1980’s. It is now agreed that digital rights management covers also other rights than copyright and even the management of such information assets, which lack legal definition. Recently several companies and organizations have published and started marketing products to manage rights in digital information. Those companies include e.g. Adobe, IBM, Apple and Content Guard. Active standardization work is happening in e.g. Open eBook Forum and MPEG. Specifications, requirements documentation and ecology papers are being

developed and discussed. We have earlier presented a framework, which defines the concept of digital rights management, its central parts, and relations between those parts. (Pitkänen and Välimäki 2000)

3.2 Many Failed Examples

Software companies tried different copyright protection mechanism in the 1980's. From hardware based solutions to software, none proved successful enough to become a standard. Now, many software companies do not use any kind of technical protection mechanism. Instead, they monitor companies using software with the help of the legal system.

Digital video was the first media type where a large-scale DRM system was implemented. The experience was not very promising: DivX standard died in 1999. The main reasons for the failure were its relatively high price, lack of real ownership to the films, its lateness to market, and the inadequate supply of popular movie titles. Disappointed users complained the format offered no real quality or price advantage and were all too wary of a Beta-VHS or Laserdisc repeat. (Patrizio 1998)

DVD format is another example of a mass-market DRM system for digital video. It managed to capture the critical mass perhaps because users hadn't real alternatives. In 1999 the system was hacked by the developers of DeCSS and the hack is now widely disseminated. After successful but too late litigation attempts, the content owners have turned considering new DRM mechanisms. In this case, the content owners seem to have two problems. On the one hand, litigation is no more possible because the user community is decentralized. On the other hand, introducing a new DRM system is difficult and costly because of the lock-in effect to current DRM technology in installed DVD-players.

3.3 Some success stories

DRM has not been a total failure, though. The music web stores like Apple iTunes, (new) Napster and 0D2 in Europe rely on DRM as a way to protect their catalogue. The content owners have demanded this as a precondition for licensing music for web distribution. The technology industry has been more sceptical on the benefits of DRM. For example Apple's CEO Steve Jobs has been publicly ready to admit that their system cannot be secure. The services have been never the less relatively successful and users have been ready to pay for the music.

Most likely one big reason for this is that the services limit user rights relatively modestly. For example, all major services allow currently burning downloaded songs to CDRs. This makes it trivial to bypass DRM, because CD-format does not include any protections. There have been in fact some arguments that the real reason why companies like Apple are ready to use DRM is consumer lock-in. As EFF's staff lawyer Fred von Lohman puts it:

"So you're Apple, and you make all your money selling iPods. You invest in the Music Store to make the iPod even more attractive, never intending to make much margin on the 99 cent downloads. But here's the problem -- you really don't want every other maker of portable digital music players to free-ride on your Music Store investment. After all, the Music Store is supposed to make the iPod more attractive than the competition.

Here's where FairPlay comes in. It's a great barrier to entry that keeps the iPod as the exclusive device for the Music Store. Competitors who dare to reverse engineer the protocols or otherwise support interoperability find themselves staring down the barrel of the DMCA." (von Lohman 2004b)"

However, one must point out that these commercially somewhat successful content distribution systems do not allow consumer distribution of the downloaded content. In short, these DRM-powered systems do not work the way P2P systems do.

3.4 DRM – has it finally arrived?

DRM has its positive and negative aspects as can be seen from table 3. It can be used to conserve the traditional business models of content industry and perhaps add some new ones. Its "law and order" approach offers security to the users and industry alike. At the same time it allegedly threatens some new forms of creativity and makes it much harder to create innovative products for new entrants (Lessig 2004).

| DRM supports | DRM complicates |
|-------------------|--------------------|
| Centralized P2P | Decentralized P2P |
| Organized Control | Virtual Equality |
| Quality and Trust | Usability |
| Commercialization | Entry into markets |
| Production | Creation |

Table 3. Supposed costs and benefits of DRM systems in P2P.

One big question is what exactly DRM protects. The examples above seem to imply that it is not necessarily the content itself. It is very hard to build a safe DRM-system, which current online music services don't even try to do. Software-based solutions will work against normal users, but power users will always be able to find cracks from the Internet, even if legislation projects like DMCA and EU directives makes it illegal to publish such

programs. Hardware-based solutions are normally too difficult for power users but there is nothing that will stop professional pirates in the end game (Schneier 2001)

| Normal citizen | Advanced user | Professional pirate |
|-----------------------------|-----------------------------------|-------------------------------------|
| No technical knowledge | Good technical knowledge | Excellent technical knowledge |
| Any protection scheme works | Software-based schemes don't work | Can eventually crack any protection |

Table 5. User capabilities and DRM

However, there are certain factors that suggest the situation is changing. In the future the relative share of handhelds with embedded software will probably grow over the general purpose PC. That means that users do not have anymore unlimited access to their system and therefore it may be possible to build a DRM-system, which would be effective in normal and advanced user groups. There is still the problem that people do not understandably want to buy products, which do not offer as high functionality and usability as the equal non-DRM products. The only solution for this is that DRM systems must offer also something added value to the users to compensate the lost functionality and usability.

4. Conclusions and levy option

From consumers' point of view P2P offers basically everything they needed except one thing - legal safety. On the other hand DRM makes their life more complicated. One has to choose, which vendors' service to support and it is very hard to avoid lock-in for both hardware and service. One can be never certain that the music they have bought can be used in their next computer or home audio system.

Content industry's position is naturally quite opposite. From their perspective the only positive thing in P2P sharing is that it is mostly illegal.³ However, it is important to note that not all artists share this point of view because P2P offers them a cheap way to reach their potential audience. DRM has been content industry's "Holy Grail" for a while because it helps them to keep their basic business model intact and only adds new possibilities like pay-per-view purchasing model.

Can the huge gap between these positions be bridged by combining P2P and DRM? Such a solution, though only academic imagination at the moment, would have indeed many benefits. The content providers can lower significantly their costs because the users take care of moving the content files around. From users perspective the benefit is that they can be more certain what they are going to get from the download. However, we haven't yet

³ Admittedly, projects like Creative Commons mean that P2P systems distribute also quality content legally

to see any mass-market system that would allow consumers to share files themselves in P2P systems and would also include some kind of DRM and licensing scheme.

There is also the possibility of new copyright legislation that would create a new compulsory licensing regime also known as a *copyright levy*. Such a “flat-fee” option has been pushed lately hard by the opponents of content industry as an option for suing the users for file sharing. In this system the content usage would be measured somehow (for example by statistical sampling) and the money collected from the users (e.g. as a part of the IPS’ fee) would be then distributed to the right holders based on this information. The system would work in the same way as the compulsory licensing works for bars and restaurants at the moment. (Netanel 2003).

In the end the right question to ask is that what is the most beneficial approach for the society as a whole. Legalized P2P would offer most likely unlimited access to most of the cultural products ever created. The problem is that new cultural production would be limited to non-commercial productions without a way to secure reasonable profit for investments. Perhaps the flat fee model would be the answer for this digital dilemma?

Acknowledgements

We would like to thank all the reviewers and commentators who have directly or indirectly shaped the contents of this article. Especially the ideas and discussions with professor Jukka Kemppinen and researcher Tommo Reti have provided us more understanding what peer-to-peer and digital rights management imply from a legal perspective.

References

- Ashcroft, John. *Digital Gridlock Announcement*. Available online at <http://www.usdoj.gov/ag/speeches/2004/82504ag.htm>. 2004
- The Digital Dilemma. Intellectual Property in the Information Age*. National Academy Press, 2000.
- Digital Millennium Copyright Act (H.R. 2281, 28.8.1998) (DMCA)
- 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. (Electronic commerce directive).
- Harmon, Amy: "Ideas & Trends: Anarchic E-Commerce; Online Davids vs. Corporate Goliaths", *The New York Times*, date, 2000.
- Hong, Theodore: "Performance", in Oram, Andy (ed): *Peer-to-Peer. Harnessing the Power of Disruptive Technologies*, p. 203-241. O'Reilly, 2000.
- Inducing Infringement of Copyrights Act of 2004, <http://thomas.loc.gov/cgi-bin/query/z?c108:S.2560>
- Lessig, Lawrence: *Free Culture*, 2004.
- Von Lohman, Fred. More on MGM v. Grokster Ruling. Available at <http://www.eff.org/deeplinks/archives/001834.php>, 2004a
- Von Lohman, Fred. *FairPlay: Another Anticompetitive Use of DRM*. Available online: <http://www.eff.org/deeplinks/archives/001557.php>, 2004b
- Menta, Robert. RIAA and Audiogalaxy Settle. Available online: <http://www.mp3newswire.net/stories/2002/agsettle.html> . 2002.
- A&M Records v. Napster, Inc., 00-16401/403, United States Court of Appeals for the Ninth Circuit. <http://www.riaa.com/news/filings/pdf/napster/napstersummary.pdf>, 2001
- Netanel, Neil. *Impose A Noncommercial Use Levy To Allow Free Peer-To-Peer File Sharing*. Harvard Journal of Law and Technology. Fall, 2003
- Newman, Ron. The Church of Scientology vs. Grady Ward. Available online: <http://www.spaink.net/cos/rnewman/grady/home.html>. 1996
- Patrizio, Andy: Video Group Snubs Divx, Supports DVD, Available online: <http://www.techweb.com/wire/story/TWB19981201S0003>. 1998.
- Pitkänen, Olli - Välimäki, Mikko: *Towards a Digital Rights Management Framework*, IeC2000 Conference Proceedings, Manchester, UK, 2000.
- Raquillet, Romain: *The Safe Harbors For Copyright Infringement*. 1999. <http://www.lclark.edu/~loren/cyberlaw99fall/projects99/raquillet/page2.htm>
- RIAA. *Press Room: Aimster Case*. <http://www.riaa.com/news/filings/aimster.asp>. 2003a
- RIAA. *Press Room: Napster Case*. <http://www.riaa.com/news/filings/napster.asp>. 2003b
- Välimäki, Mikko - Martikainen, Petri: *Online Intermediary Liability Framework*, EMMSEC conference proceedings, Madrid, 2000.