Noise Wars: Is the Answer to the Machine in the Noise?[1]

Nicklas Lundblad
nicklas@acm.org
St Anna Research Institute
C/o Stockholm Chamber of Commerce, Box 160 50, 103 21 Stockholm

Abstract

In this article we study the phenomenon of noise files, that is: files that are low-quality or harmful to the user in any way, and how the use of these files might be designed to disrupt the functioning of peer-to-peer networks. The aim of this study is to examine legal aspects of these coming 'noise wars' and how they will affect the networks. The perspective taken is that of architecture regulation – the idea that code is law, as launched by Lawrence Lessig in *Code and Other Laws of Cyberspace* (Basic Books 1999)

Introduction

Legislation, technical measures, court cases and publicity campaigns seem all to have failed to stop the technologies of file-sharing. The copyright holders find themselves in a rapidly changing environment, once again, due to the introduction of new technologies.[2] Are there any

---

[1] To be presented at BILETA 2003, London, 14-15.4 2003.

[2] This is not a new phenomenon. See for example Allan, S, Green, S, Friedman, J, Harrington, B and Johnson, L "New Technology and the Law of Copyright:

possible means left available to try to disable these systems. The music industry might be re-reading Charles Clark's old adage "The Answer to the Machine is in the Machine", but instead of finding ways of supporting information and content commerce they could now pursue strategies of disruption.[3]

One possible such strategy is to introduce large quantities of files that do not work, or work differently, in the networks in an attempt to disrupt the functioning of the file-sharing systems. In this paper we examine the possible avenues for a music industry on the retreat, and exemplify in a mini-case study of the release of pop artist Madonna's latest single "American Life".

The paper is divided into three parts: first we introduce a history and a model of peer-to-peer networks then we discuss the strategy of noise wars and its legal implications. Lastly we examine a short case study of noise files, and give some real-world examples.

Method

This work examines the phenomenon of noise files as an attempt at architecture regulation, or an attempt at changing the code at the content layer in the three layered network model introduced by

---

Reprography and Computers" in Bush, George *Technology and Copyright: Annotated Bibliography and Source Materials* (Lomond Systems 1978) Originally in *UCLA Law Review* 15:993-1028 1968 about the introduction of the photocopier.

[3] See Clark, C 'The Answer to the Machine is in the Machine', in: P. Bernt Hugenholtz (ed.), The Future of Copyright in a Digital Environment, The Hague: Kluwer Law International

Lawrence Lessig in his *The Future of Ideas: The Fate of the Commons in a Connected World* (Vintage Books 2001). In this model the physical, logical and content layers of the Internet and information technology architecture are layers potentially open to regulation in different ways, and Lessig uses this distinction to open a discussion on control and freedom flowing from the architecture.

The hypothesis is that what we are seeing now is an attempt at architecture regoluation at the content layer, but that this will ultimately prove to be useful only to a certain category of peer-to-peer networks, as specified below.

Legal aspects of this attempt at architecture regulation are also introduced and discussed briefly.

Architecture regulation is used loosely as a term to connote the different theories on the importance of technological architecture in the regulation situation, and it is not claimed that this is an established theory – it is however claimed that it is a useful perspective that merits further investigation.[4]

---

[4] In *Code and Other Laws in Cyberspace* (Basic Books 1999), Lawrence Lessig discusses and formulates a series of interesting observations about the way code and law interact. This is later then picked up and developed by Stuart Biegel in *Beyond Our Control: Confronting the Limits of Our Legal System in the Age of Cyberspace* (MIT Press 2001).

Three generations of Peer-to-peer networks

Peer-to-peer networks are really not new at all, and the basic model offered in the networks is not technologically complex, but these networks have still had an enormous importance for the development of the legal discourse on law, information technology and the Internet.[5] Here I would like to sketch first a short history of these networks, and then I would like to present a short model of them to be able to discuss a number of observations about these networks that go the core of our study: the nature of architecture regulation.

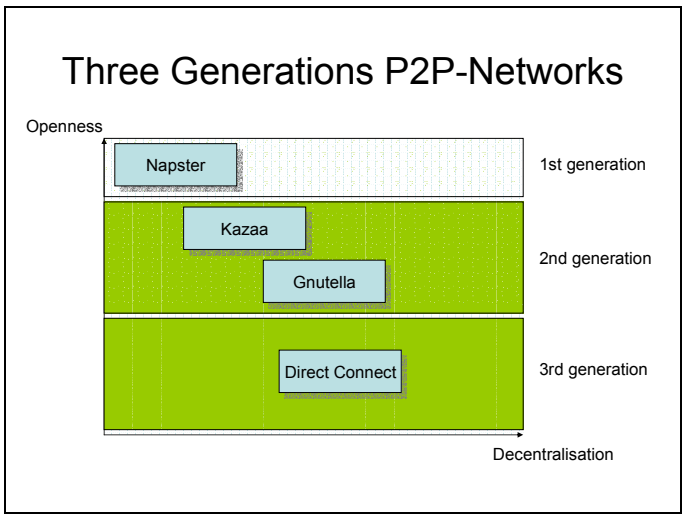

Fig 1. Three Generations P2P-networks

[5] Especially together with the developed and highly usable mp3-format. Carey, Mark and Wall, David (2001) "MP3:The Beat Bytes Back", *International Journal of Law, Computers & Technology*, Vol 15, No.1 35-58, for essays on Peer-to-peer in general see Oram, Andy, red (2001), *Peer-to-peer : harnessing the benefits of a disruptive technology*. Cambridge, MA: O'Reilly.

I argue here that the file-sharing networks can be seen as having evolved two generations, with a total of three generations, from the original generation: Napster. There were peer-to-peer networks before this, and it should be emphasised that we are not speaking primarily of technological evolution, but rather of social and legal evolution. In short, I argue that we see the following evolution:

Generation	**Architecture**	**Content**	**Control point**
1st (Napster)	Centralised	Music	Central server / Company
2nd (Kazaa)	Distributed – open	All	Internet operator
3 (Direct Connect)	Distributed – closed	All	Possibly Internet operator

The three generations also exhibit different architecture regulation effects, but this will be discussed below.

The Napster generation

Napster was – in many ways – both a genial and extremely stupid construction. The genius of Napster was obvious: it connected with a social practice that was in dire need of technological support: music sharing. The stupid decisions were to only share music and to craft the system so that there was a central control point in the form of both a

server and a company. Napster highlighted the economic and technical problems facing copyright in the information society.[6]

Napster is legendary, and it is worth examining the features of the program to realize why. When using Napster the user only needed to search for a certain file and the program then delivered a list of results that could be browsed. The results also listed the other users, and thus the user could list all files with one user to be able to browse what others had on their hard disks. This enabled a primitive form of social filtering, where it was possible to see what people who seemed to share my music taste listened to that I had never heard about.

This was an interesting feature, and it enabled the user to find both new chatting friends (there was a built-in chat function) and new music.

---

[6] For an economic analysis see Yen, A (2003) "A Preliminary Economic Analysis of Napster: Internet Technology,Copyright Liability, and the Possibility of Coasean Bargaining" in *University of Dayton Law Review* (forthcoming), for a general view on copyright in the information society, with a focus on economic aspects, see also the more spectacular Barlow, John Perry "The Economy of Ideas" *Wired* Mar 94.

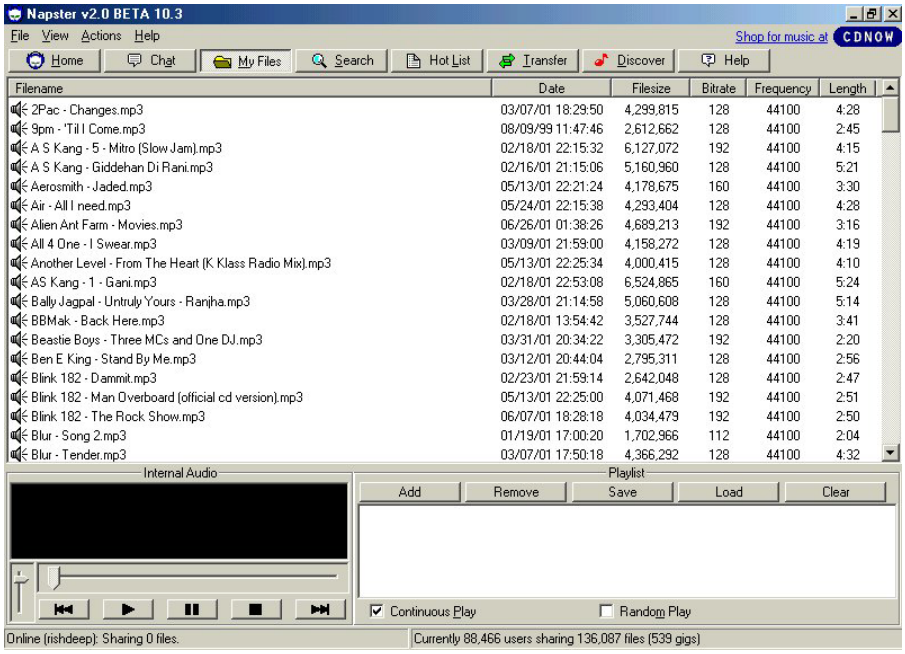

Fig 2 Napster – early version

The software was dedicated almost solely to music. In retrospect that seems odd, but it could be defended. At the time when Napster rose to fame the bandwidth was not such that it was realistic to download extremely large files. When the bandwidth increased the next generation file-sharing programs could easily move on to films and software.

Napster was efficiently disabled by the lawsuit brought against it.[7]

---

[7] For an analysis of that case see Carroll, M (2002) "Disruptive Technology and Common Law Lawmaking: A Brief Analysis of A&M Records, Inc. v. Napster, Inc." Villanova Sports and Entertainment Law Journal, Vol. 9, No. 5, 2002.

Kazaa, Gnutella and Freeenet

The second generation peer-to-peer software grew up in the shadow of the lawsuits that Napster had generated. They learnt from this and constructed architectures that were "pure" peer-to-peer, and without central control points in company and software.[8]

Kazaa – probably one of the most popular pieces of file-sharing software – was developed by a company, but stopping the company had not stopped the file-sharing networks that it had helped develop.[9]

The two other examples of the second generation are completely open and in a sense uncontrollable architectures.

Gnutella is one of the most well-known open source file-sharing project, and it was developed as a reply to the many lawsuits against other file-sharing applications.[10]

---

[8] Although it has recently been revealed that Kazaa does have something called super nodes in the network and that the company behind Kazaa actually hosted such a node for a while. See Jesdanun, A "Internet file-swapper frustrates entertainment industry" L.A. Daily News (http://www.dailynews.com/Stories/0,1413,200~20950~1151514,00.html[2003-04-07])

[9] Kazaa boosts, according to its website, 211 million downloaded clients. (http://www.kazaa.com [2003-04-10])

[10] In fact, there is no one Gnutella, but several different pieces of client software that work in different ways.

This generation moved away from the central control point, even though it is still possible in the case of at least Gnutella and Kazaa to argue that Internet Service Providers have a theoretically possible chance of monitoring traffic and catching the individual users that traffic in copyrighted files.

Freenet addresses this issue and it is a very conscious strategy. Freenet was also developed as an encrypted traffic network in which it would not be even possible for any third party to see what files flowed between the nodes in the network.[11]

Direct Connect

Direct Connect[12] and other similar models[13] are interesting because of what they are not. They are not large-scale file-sharing networks, but

---

[11] Freenet was also developed in strong opposition to copyright, and a very conscious opposition at that. In the Frequently Asked Questions section there is a philosophy page that states the following: "8. And what of copyright? Of course much of Freenet's publicity has centered around the issue of copyright, and thus I will speak to it briefly. The core problem with copyright is that enforcement of it requires monitoring of communications, and you cannot be guaranteed free speech if someone is monitoring everything you say. This is important, most people fail to see or address this point when debating the issue of copyright, so let me make it clear: You cannot guarantee freedom of speech and enforce copyright law. It is for this reason that Freenet, a system designed to protect Freedom of Speech, must prevent enforcement of copyright."(http://freenetproject.org/tiki-index.php?page=Philosophy[2003-04-10])

[12] See the Neo-Modus website (http://www.neo-modus.com/[2003-04-10])

[13] See for example this simple FTP-based solution http://www.clientbackup.com/.

rather small closed node networks in which trusted parties exchange files without being bothered by the others. If the other two generations have been open networks, Direct Connect and other similar solutions are more like the *splinternets* envisioned by Clyde Wayne Crews. Crews wrote a famous article in which he suggested that we need more Internets rather than more regulation for the Internet.[14] He also stated that we will see such a social segregation into smaller networks, splinters of the Internet, or splinternets, and that these networks will become more and more important in the near future.

The development embodied by applications like Direct Connect will prove crucial for the development of file-sharing as such, and the legal discussion of this phenomenon. These semi-private networks will be much harder to access and control than any other previously used technology. These networks are not *open* and thus they are not possible to monitor in the same way one monitors the already open networks.

A Basic Model

There is much to be said for addressing the problems of peer-to-peer networks on not a legal level, but rather on an architecture or technology level. There are several different possible ways to control the file-sharing networks, and it is useful to work with a model of these networks to see how the different methods can be justified and studied. There are also a number of important lessons to be learnt from modelling the networks that we will return to.

---

[14] See Crews, C "One Internet Is Not Enough" TechKnowledge Issue #3 April 11, 2001 (http://www.cato.org/tech/tk/010411-tk.html82003-04-07])

In this section the concept of noise will be studied and used to explain one possible avenue of attack open to the copyright holders. Before the idea of noise warfare is introduced we need a model of file-sharing networks to begin with, and to use as a starting point for our studies.

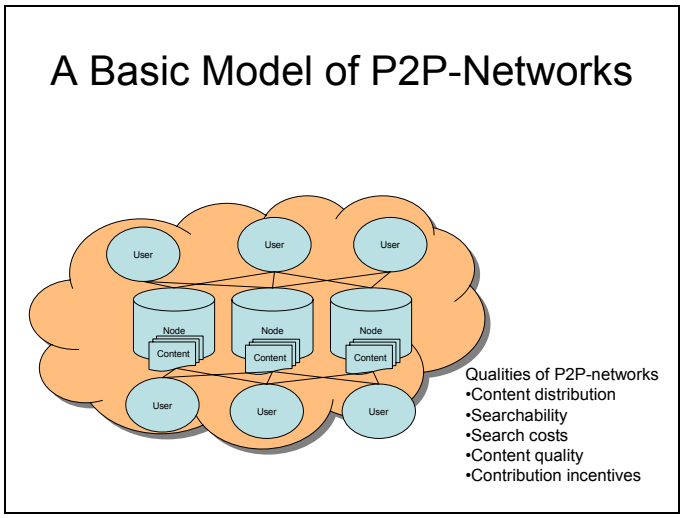

Fig 3 A basic model of P2P-networks

File-sharing networks can be schematically represented as a semi-formal model consisting of the following different components:

- *Users* (People downloading and using the systems)
- *Content* (The files accessible in the system)
- *Nodes* (Connected computers in the file sharing network)

We can then describe a number of basic variables that are useful to have at hand when discussing file-sharing networks.

(1) *Content distribution*. The distribution of files in the network over nodes. A content distribution is a list of files and the nodes they reside on. This concept has important effects when discussing

the vulnerability of these networks. If, for example, a single node has all the content, and all other nodes simply download from this content node, then the network is fairly easy to cripple: attack the one node!

(2) *Searchability*. The ability for users to find the content they want. If the network lacks this basic property it is even possible to question if it is indeed a network at all.

(3) *Search costs*. These costs are costs associated with finding content in the network. Networks that are searchable are not necessarily searchable in a manner that is cost-effective, quick and simple. This variable shows what the average search cost is.

(4) *Content quality*. This is a variable that shows what the average quality of the content in the network is. If we are speaking about music files, this would typically be the quality of the average music file found in the network.

(5) *Contribution incentives*. This is the mechanism constructed in the networks to ensure that there is a flow of contributions to the file-sharing network. This might be both something encoded in architecture, and something wholly related to the nature or social significance of a certain network. Contribution incentive mechanisms in different networks are shown below. It should be noted that there are several different ways of constructing these mechanisms, and that they are prime examples of architecture regulation. They represent examples of how the architecture of file-sharing networks is constructed to ensure participation.

(6)

Software	Contribution Incentive Mechanism	Social Model	Result
Napster	None	Altruistic model	Uneven content distribution
Kazaa	Number of files shared and rated affect download speed and priority.	Egoistic model	Rated files
Gnutella	None (variable – open source)	Altruistic	Uneven content distribution.
Direct Connect	Gigabytes shared can be set to work as keys to access to the larger semi-open nodes.	Commitment model	Large sets of data (but not necessarily qualitative sets)

These different concepts are both important and useful in an anlaysis of peer.to-peer networks. We will return to this model in the following sections where different examples of architecture regulation and attempts at architecture regulation are developed.

Attacking the networks

From the basic variables and the simple model introduced above we can sketch some very simple strategies of attacking file-sharing networks that work with architectural features of these networks.

Firstly, it depends on the *content distribution* in the networks. If the networks exhibit a number of high content density network nodes, i.e. a few very large nodes that do much of the storage of files, then attacking

these would be a reasonable way forward.[15] These network nodes could then be attacked with massive traffic attacks or perhaps even with DoS-attacks.[16]

Secondly, it is possible to attack the architecture by emitting massive amounts of low-quality files that lower the over all content quality of the network. This could be accomplished by simply changing the names of some of the most popular files, or by distributing files that are low quality/noise filled.

Thirdly, hostile code could be implanted in files that purport to be music or films. It could be possible to attack the users of file-sharing networks by simply infecting their computers with viruses that erases mp3-files for example.

In this section we will examine the second and third methods more closely.

---

[15] As it turns out this is indeed the case. In Adar, E and Huberman, B "Free Riding on Gnutella" First Monday, volume 5, number 10 (October 2000) (http://firstmonday.org/issues/issue5_10/adar/index.html[2003-04-07]) the authors show that 70 percent of the users of Gnutella only download – that is: 100% of the content is on 30% of the nodes.

[16] See Daswani, N and Garcia-Molina, H "Query-Flood DoS Attacks in Gnutella" *Proceedings of the 9th ACM Conference on Computer and communications security 2002,* November 18-22, Washington, DC, USA.

Information, Noise and Value

Information and noise are basic categories of informatics, dating at least back to the seminal paper by Claude Shannon on mathematical information theory.[17] These terms have since become every-day concepts, but they have also changed and become less strictly defined.

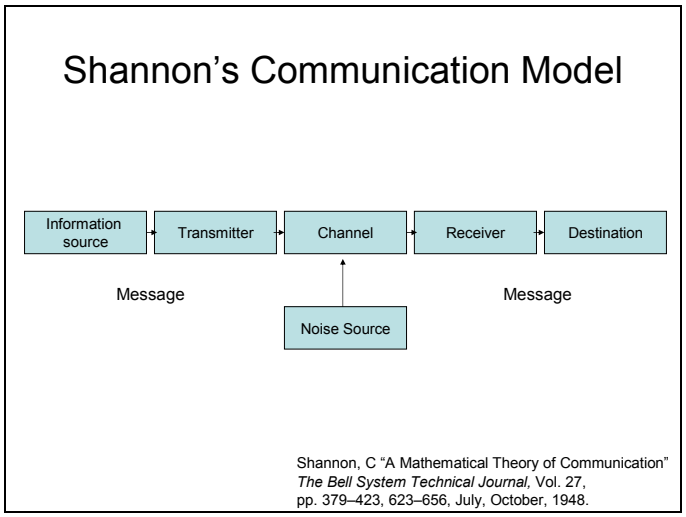

Fig 4 Shannon's communication model

The Shannon-model is very simple, and serves as a good prototype for the questions that will be discussed in this paper, but it should be noted that I do not propose to use the terms in their strict mathematical

[17] Shannon, C "A Mathematical Theory of Communication" *The Bell System Technical Journal,* Vol. 27, pp. 379–423, 623–656, July, October, 1948.

definitions. I rather think that they should be seen as general concepts in the way Henry Perritt seems to view them:[18]

> The next question is whether intelligent systems can be used to improve the signal to noise ratio. When electrical engineers speak about the signal to noise ratio, they refer to how distinct the desired information is from background noise. Extending the idea to the Internet, one perceives higher signal to noise ratio when pertinent messages are not obscured by spam and random information not of interest to the particular user. Today's Internet has a number of applications intended to increase the signal to noise ratio. The World Wide Web itself assists users in focusing their attention and computing resources on material in a particular area, sparing them the necessity of downloading and reviewing much irrelevant material in order to find the desired items. Internet newsgroups and mailing lists perform a similar function with respect to interactive discussions. The signal to noise ratio isse thus overlaps concerns about improving search and retrieval precision and efficiency, and also overlaps ongoing efforts to define electronic communities more precisely.

Perrits definition is useful for the task undertaken here – to understand how noise can be used to regulate peer-to-peer networks.

Noise Content – a Taxonomy

There are different ways of creating noise in the file-sharing systems. It is useful for our continued examination to establish a simple taxonomy of such files. In the following section we examine three different examples of what could be called noise content or noise files.

---

[18] Perritt, Henry H Jr "Mapping the Information Superhighway" in International Journal of Law and Information Technology Vol 3 no 3 Winter 1995 (pp 201-213) p 210)

Misnomers

Misnomers are files that are named incorrectly. A filename usually represents the content of that file and if the file name is constructed to consciously mislead the users of a certain file-sharing service, then that constitutes a form of noise.

Misnomers can be divided into two different categories: those that are misnomers in the sense that they are still valid and functioning files, but not the files that one would be lead to believe from their names. A case in point might be a file that is named brucespringsteen-borninamerica.mp3 and when played plays Madonnas *Bedtime Story*. This is an example of a *copyrighted misnomer*. The downloading and copying of the file might still be considered reproduction, and the rights that are attached to the work in question might still be infringed, but they have been infringed involuntarily by the user who actually intended to download material, but not that material.

We could also have a case where the file downloaded purports to be copyright material but actually is non-copyrighted material/material in the public domain. Such *public domain misnomers* are still interesting, but they present less of a legal problem (see below).

Distortions

Another example of noise content would be files that have been manipulated and distorted in some way. There are plenty of examples in the file-sharing networks today:

- Click files where loud clicks are heard when the files are played back.

- Looping files, where a single part of a file is looped indefinitely.

- White noise files, where significant levels of white noise have been inscribed in the file.

All these are examples of files that are correctly named, but worthless noise files.

Malicious Code

The third category is slightly more worrying than the preceding ones, since we in this category find files that can be classified as malicious code. These files in fact are crafted with the intention of controlling and/or destroying information on the recipient's computer. There are plenty of examples:

- Files containing viruses.

- Files containing scripts that affect the functionality of the computer in question.

- Files that report on the content of the computer to monitoring authorities.

- Files that download other kinds of malicious code.

All these files are recognized by the fact that they intend to reduce the functionality of the computer where they reside. These kinds of files must, however, also be divided into two different subcategories:

- Files claiming to be legitimate files

- Files that are already likely to be illegal to copy and/or download.

This distinction will turn out to be interesting in trying to assess the legality of this approach.

Berman Laws

There are those who argue that it might be illegal today to combat file-sharing networks with noise files or hacking, but that it should be allowed in the future. One of the strongest proponents for this point of view is Howard Berman, congressman in the United States. In 2002 he sponsored a special bill, the so-called peer-to-peer privacy prevention act. Berman's bill is a new form of law that is relevant in the context of architecture regulation. Berman himself, in the introduction of the act, makes this clear:[19]

> One approach that has not been adequately explored is to allow technological solutions to address technological problems. Technological innovation, as represented by the creation of P2P networks and their subsequent decentralization, has been harnessed to facilitate massive P2P piracy. It is worth exploring, therefore, whether other technological innovations could be harnessed to combat this massive P2P piracy problem. Copyright owners could, at least conceptually, employ a variety of technological tools to prevent the illegal distribution of copyrighted works over a P2P network. Using interdiction, decoys, redirection, file-blocking, spoofs, or other technological tools, technology can help prevent P2P piracy.
>
> There is nothing revolutionary about property owners using self-help -- technological or otherwise -- to secure or repossess their property. Satellite companies periodically use electronic countermeasures to stop the theft of their signals and programming. Car dealers repossess cars when the payments

---

[19] Berman, H "Introduction of the Peer to Peer Piracy Prevention Act (2002 25th July) (http://www.house.gov/berman/floor072502.htm[2003-04-01])

> go unpaid. Software companies employ a variety of technologies to make software non-functional if license terms are violated.
>
> However, in the context of P2P networks, technological self-help measures may not be legal due to a variety of state and federal statutes, including the Computer Fraud and Abuse Act of 1986. In other words, while P2P technology is free to innovate new, more efficient methods of P2P distribution that further exacerbate the piracy problem, copyright owners are not equally free to craft technological responses to P2P piracy

Berman is correct, in a manner of speaking, in that some of the measures that he describes may not be legal in the US, and this is probably true also for the European Union member states. But what, then, does he suggest? The answer is thought-provoking:[20]

> Through the legislation I introduce today, Congress can free copyright creators and owners to develop technological tools to protect themselves against P2P piracy. The proposed legislation creates a safe harbor from liability so that copyright owners may use technological means to prevent the unauthorized distribution of that owner=s copyrighted works via a P2P network.

Here we see the unique quality of the Berman Bill, and thus also of a possible class of laws that I will term *Berman laws*. These laws are simply laws that open up for attempts at architecture regulation by exempting the parties engaging in architecture design from laws that govern the regular users of the new technologies. This is unprecedented, and has

[20] Berman 2002

received heavy criticism from Net libertarians in the Electronic Frontier Foundation:[21]

> The EFF agrees with Rep. Berman that, like the rest of us, copyright owners are entitled, within the bounds of the law, to use technological self-help measures to protect their assets. No legislation is necessary for that. What the Berman P2P Bill does is permit copyright owners to go further and violate the law. This unprecedented power has never been granted even to law enforcement, much less to a single industry.

The EFF:s position is quite understandable, but they idea of legislating safe harbours for what would otherwise constitute illegal behaviour is still quite interesting. Berman laws, should they become more common, will have a profound impact on the way we view architecture regulation. Architecture regulation might – in a world with Berman Laws – become more like war: sanctioned by the state on the offenders by the rights holders.

Responding to Noise – Rating Solutions

The fight for domination of the file-sharing networks is not one-sided. If the music industry or interests close to that industry decide to fill the systems with noise, the file-sharing interests retaliate by introducing different noise dampening technologies. It is even possible to build reputation-based peer-to-peer networks.[22]

---

[21] "The Berman P2P Bill: Vigilantism Unbound" EFF (http://www.eff.org/IP/P2P/20020802_eff_berman_p2p_bill.html [2003-04-01])

[22] Damiani, E, Vimercati, D, Paraboschi, S, Samarati, P, and Violante, F "Peer to peer networks: A reputation-based approach for choosing reliable resources in peer-to-peer

The noise dampening technologies can be divided into different categories:

- Rating services and solutions. Different rating solutions ensure that files that are low in quality do not disseminate through-out the network. We will look into this in more detail later in this section.

- Access conditions. In software solutions like direct connect the access control can serve to control that the networks are not filled with noise. Users that deliver noise files can be kicked more or less from the nodes where they have disseminated these files.

- Self-regulation. False files are removed from users hard disks because they just take up space. They are continuously deleted if the users have the time

These different strategies for dampening the noise in the networks can be quite effective and help preserve the value of these networks for users. It is far from obvious whether or not they are a stable solution in the noise war however. There are a number of problems that have to be examined to establish if these systems will be effective.

Firstly, users have to be given a clear incentive to rate the different files. In Kazaa this is accomplished by connecting the number of rated files to the downloading speed. Kazaa claims that the users will achieve a

---

networks" Proceedings of the 9th ACM conference on Computer and communications security November 2002

higher probability of getting access to files and a prioritized downloading schedule if they rate their files:

In the particular case of Kazaa there are three participation levels, and they are determined partly by the number of files shared, but also by the number of files rated:[23]

> Low - you download more megabytes from other users than other users download from you. The files downloaded from you are probably not integrity rated.
>
> Medium - you allow a solid amount of megabytes to be downloaded from you, or a healthy amount that are integrity rated. Or you have just started and not done much yet.
>
> High - you allow more megabytes to be downloaded from you than you download from other users. You are really doing your bit.

Note also that the participation levels are determined by the information flows, i.e. if you download more from others than they do from you, your participation rate will sink over time.

The integrity ratings are easy to do. In the library section of Kazaa where all the files are catalogued one simple right-clicks on the file in question and gives it a rating.

---

[23] Book of Kazaa (help file): Participation levels

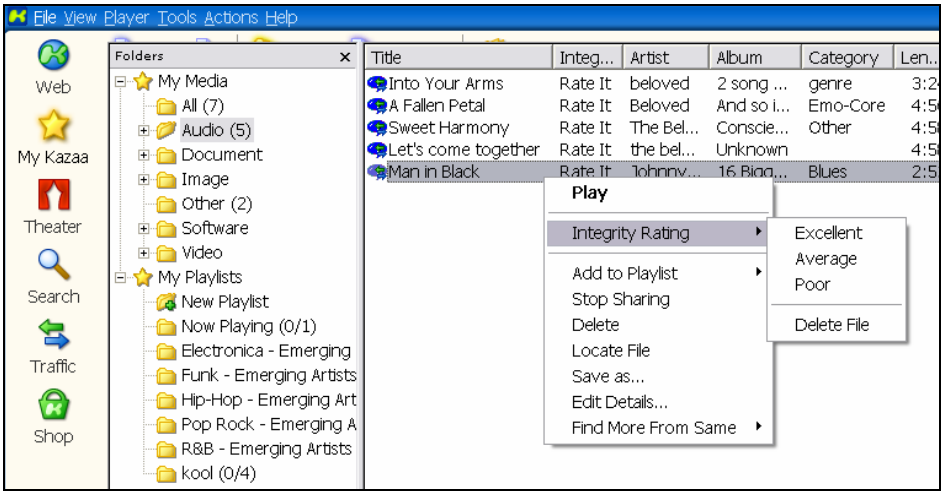

Fig 5 Kazaa and rating

Note also that the integrity rating has been coupled with the deletion option to enforce and simplify the self-regulatory functions described earlier.

Legal analysis of Noise

Is it lawful to combat the peer-to-peer networks in this way? This is far from an easy question to answer. In this section we will concentrate on the different legal aspects and try to sketch a set of legal scenarios and try to determine the legal status of some of these scenarios.

Fraud

In some cases it will be relevant to ask if the use of misnomers, distorted files and malicious code constitutes fraud.

The conditions for fraud are different in different countries. The main criteria are that someone has gained something by defrauding someone else with the intent of doing so.

In rare cases this description may fit at least misnomers. Consider the case where someone misnames their own, unknown material so that it looks as if their material is the latest single from a famous artist. In this case they will have intentionally defrauded you, and they have gained time and a marketing effect, and you have lost time, and a certain amount of connection and downloading resources.

It is however highly unlikely that any court would admit such a claim, considering that the original intention of the defrauded was to commit a crime, and the involved values are infinitesimal.

Moral Rights

It seems obvious that misnomers of different kinds might infringe on moral rights. As we have seen above the Berne convention defines moral rights in article 6 bis:

> (1) Independently of the author's economic rights, and even after the transfer of the said rights, the author shall have the right to claim authorship of the work and to object to any distortion, mutilation or other modification of, or other derogatory action in relation to, the said work, which would be prejudicial to his honor or reputation.
>
> (2) The rights granted to the author in accordance with the preceding paragraph shall, after his death, be maintained, at least until the expiry of the economic rights, and shall be exercisable by the persons or institutions authorized by the legislation of the country where protection is claimed. However, those countries whose legislation, at the moment of their ratification of or accession to this Act, does not provide for the protection after the death of the author of all the rights set out in the preceding paragraph may provide that some of these rights may, after his death, cease to be maintained.
>
> The means of redress for safeguarding the rights granted by this Article shall be governed by the legislation of the country where protection is claimed.

As anyone can see both misnomers and distortions seem to be in breach of p (1) in the article. The question is of course if the right to claim authorship should be seen as a right to always be named as the author of a specific work. Or if this is a right that is only interesting where claimed.

The distorted files seem to offer a simple example. These files, as far as the original file is at all recognizable, are clearly examples of infringing the moral rights. The distortion is clearly a derogatory act, making the works sound unprofessional and noisy.

Computer Intrusion

In cases where type III noise content is used and viruses planted or any other such malicious code inserted into a computer network, this could clearly constitute computer intrusion or any other form of computer crime.

Eroding the Value of Networks

An interesting issue is if someone who intentionally floods a file-sharing network with noise content can be held responsible or liable for the erosion of value in the network as such. There is clearly such erosion, and users will experience a reduction in value, but it is of course highly doubtful if this is actionable. The whole question seems to hinge on whether or not the networks can be said to be a value that someone has a legitimate right to, and that has simply not been shown.

Contractual and Licensing Problems

A more pressing issue is if the flooding of the systems constitutes any form of breach of the software licenses under which the file-sharing

software is licensed. In the case of Kazaa the license contains a number of provisions under which it could be deemed illegal to distribute noise content. It is useful to examine this in detail:

> 2.1 Transmit or communicate any data that is unlawful, harmful, threatening, abusive, harassing, defamatory, vulgar, obscene, invasiveof another's privacy, hateful, or racially, ethnically or otherwise objectionable;

It could be argued that noise content is both unlawful and harmful in different ways. In the case of malicious code this is obvious, but also in the case of misnomers. If the misnamed file is copyrighted, its distribution is prohibited not only by law, but also under this license.

> 2.4 Forge headers or otherwise manipulate identifiers in order to disguise the origin of any data transmitted to other users;

Clearly this also addresses the issue of misnomers and distortions. Misnaming is disguising the origin of data, since it seems to claim that the data in question is what it is not.

> 2.6 Transmit, access or communicate any data that infringes any patent, trademark, trade secret, copyright or other proprietary rights of any party;

This, again, seems to make the transmission of misnomers a breach of the license.

> 2.7 Transmit or communicate any data that contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment;

Clearly, malicious code of different varieties is directly prohibited by this clause.

> 2.9 Interfere with or disrupt the Software;

This could be construe to mean decreasing the value of the network of the software by introducing large amounts of noise content.

> 2.13 Modify, delete or damage any information contained on the personal computer of any Kazaa Media Desktop user; or
>
> 2.14 Collect or store personal data about other users.

These two clauses directly address malicious code, and seem to exclude that possibility for anyone interested in using the more drastic methods of disseminating viruses in this community.

It might be argued that it is ridiculous to claim that the license prohibits the use of noise content, when it also prohibits the transmission of copyrighted files – a practice that is deeply entrenched in the file-sharing community.

Rating Solutions and Legal Interpretations

Rating solutions raise new legal issues. It is legitimate to ask whether or not the action of rating a file constitutes an infringement of copyright in any way. The question is relevant, since rating is a practice that increases the efficiency of the file-sharing network, and this generates a directly quantifiable loss for the rights holders.

If it would be possible to point at a certain volume of file-sharing that would be possible without rating and another, larger, volume that would be likely with rating systems, then there is an actual financial loss for copyright holders that results directly from the practice of rating the different files on ones system.

It seems obvious that rating files that are in the public domain present no problem. The intentional rating of pirated files is however more

problematic. Is this aiding and abetting in copyright infringement? Possibly, but it seems hard to find any legal description that could fit the description of rating practices, and it seems reasonable to assume that they are legal.

The legal analysis clearly shows that noise is hard to classify as a legal phenomenon, and this in itself is an indication of an architectural phenomenon. Noise is in a sense an architectural phenomenon, created by copyright holders – and as such it must be studied closer.

Noise as Architecture Regulation

In following Lawrence Lessig's approach to law and information technology, it is, as mentioned above, useful to study noise files as a form of architecture regulation in the content layer. In Lessig's now wide-spread model of regulation four factors interrelate: laws, norms, markets and architecture. I will propose that noise is a form of architectural regulation because it builds not on law, norms and markets but rather on an inherent weakness in the architecture content layer of the file-sharing networks – an architecture that allows anyone to contribute. Noise wars are possible because of the architecture.

But does that make sending noise files into the file-sharing networks an example of architecture regulation? I would argue that it does. Noise content is also code, and it is code that flows in the architecture – architecture within architecture if you will. And using noise content is designing and implementing a feature in the architecture of the file-sharing networks.

We can show this both by analyzing the issue in an economic framework, arguing that architecture regulates by imposing cost structures on users

Economic analysis

Economically, what happens is this. The noise content raises the *search costs* in the network, and by changing the cost structure imposed on the user in this way it has a purely regulative effect. It might even eradicate *searchability* entirely.

This is obvious, but it is also clear that noise content actually increases the costs not only of the downloaders by making it less likely that a given file is indeed what it purports to be, but also by forcing different rating schemes on them that consume both time and resources.

The cost structure that affects a user, then, is this:

- Costs for searching for files in a network where the increasing number of files increase search times and search costs.

- Costs for evaluating the found files and to determine if they are regular or noise content.

- Costs for rating files in order to keep the participation level that enables the user to download files at an optimal speed.

- The expected sanction costs for offering files for download in order to be able to download or join networks. Calculated as the cost of the sanction times the probability of getting caught.

- Costs for virus infections. These are the costs closest to enforcement costs in the file-sharing networks. They are easily calculated as the cost of virus infection times the probability of such an infection.

These costs become higher or remain constant when the level of noise in the system is increased (the possible exception is the expected sanction cost for the user offering noise files). The regulative effect of introducing noise is thus probably a decline in usage. It might even be theorized that there is a point – a noise point – at which the expected value of the content in a network is exceeded by the expected aggregated costs above and searchability disappears. At this stage the network itself is transformed into noise, it looses its value and becomes worthless for the individual user.

A Case Study – American Life by Madonna

American Life is the recent single by singer and pop artist Madonna. This single has been the object of one of the most successful noise campaigns in file-sharing history so far. The strategies and technologies of this campaign are valuable for studies in the art of noise warfare.

What anyone would do if they were interested in this song would be to search for Madonna or American Life in for example Kazaa. This would give a result list very much like this one:

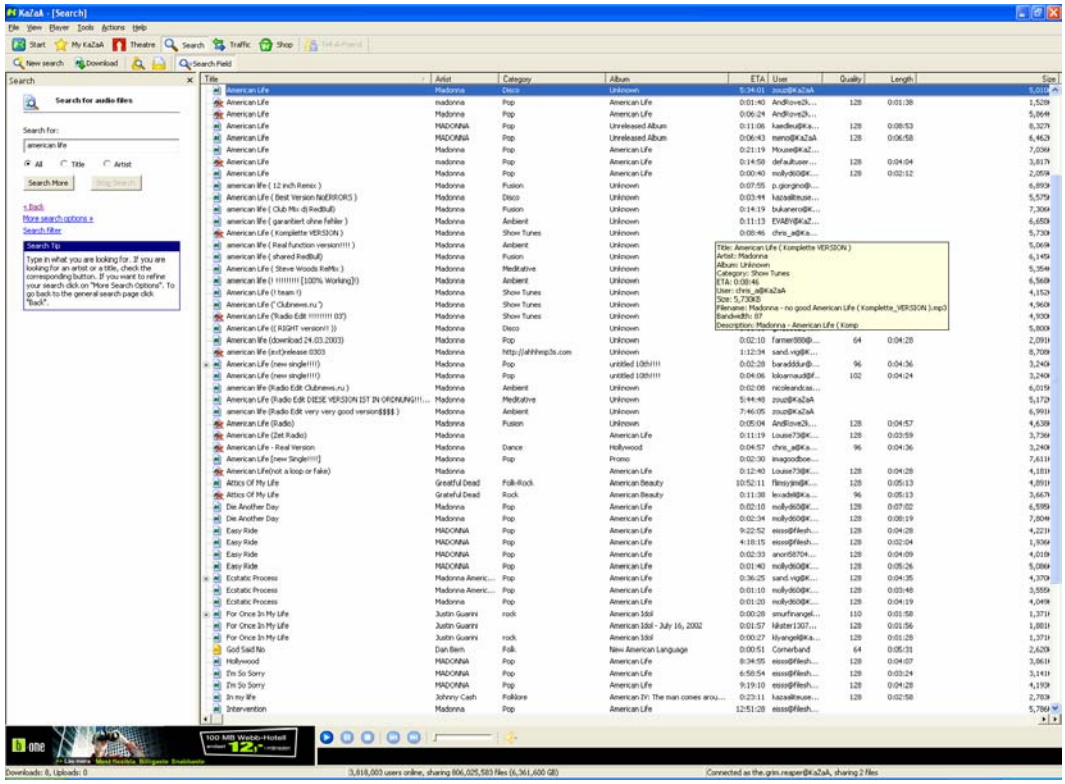

Fig 6 Kazaa search results

The user in question would then try to download any or all of the files named American Life to get access to the music without paying.

How, then, can this be stopped? One way would be to flood the system with false files – decoys – and thus increase the noise levels. One does not need to disseminate very many of these, but rather only a handful and then let the magic of file-sharing do its work.

The dissemination rate of new music is quite fast, and the end result would be considerable dissemination of the decoys. But how should then these decoys be designed?

One of the best decoys I have seen so far is the following decoy (madonna-American Life-american life.mp3) that contains a sample of

Madonnas latest song *American Life* looped again and again. The file sounds like Madonna, and the loop is seamless. The end result is a slightly boring, but not totally unbelievable Madonna-decoy. The repetetive structure is clearly visible in this wav-format rendering:

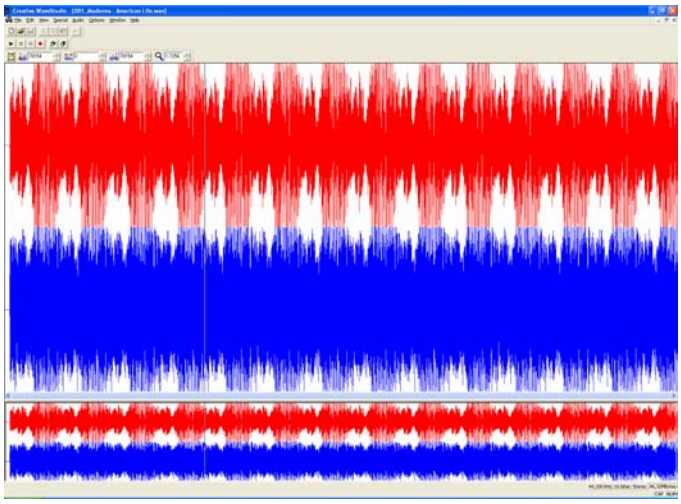

Fig 7 Wav-analysis of noise file

The creators of this decoy have also been intelligent enough to realise that the file size counts as a unique identifier in most filesharing networks, and they have thus created the same loop file in different lengths and sizes. So, for example, the file (2_Madonna_-_American_Life.mp3) is the same type of file but rather than 4:57 it is 5:02 minutes long. There are versions from 3 minutes up to 5. This introduces considerable noise in the system, since filesizes are the basis of rating services in Kazaa.

This is much better than the other version of the same decoy (Madonna - American Life (very_very_good version$$$$).mp3), which plays what sounds like an advertising jingle for a latte over and over again. Many of the files have the same kind of message in their name:

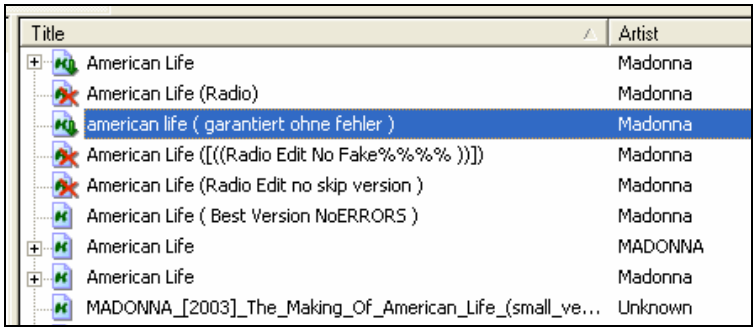

Fig 8 Different file names

Another file (Madonna-American Life-american life-Good One.mp3) simply contains a recorded message from Madonna[24] where she says: "What the fuck do you think you're doing?". This is an attempt at upbringing and it gives pause to the listener, who is probably supposed to reflect on his or her moral values.

The Madonna campaign also features all the new songs from her coming album, and these songs are all different lengths of the aforementioned looped file. This is really interesting, since there is a marketing effect involved here as well. Not only does the parties behind this campaign stop download, they also market the new albums and the songs on it.

Now, will this strategy be successful? It is successful right now. None of the files on the list that was presented above is the true song. The system is completely filled with noise as of now. But will this last? Probably not. After a certain time the system adjusts and fills upp with content that is not noise.

[24] Or what sounds remarkably like Madonna.

Still, it could make economic sense to use this kind of tactic to delay the dissemination of the content. The main question is how a typical sales diagramme would look. If we imagine a sales process in which the bulk of the sales come at an early stage, each day of delays could be worth quite much. Consider the following possible sales curve:

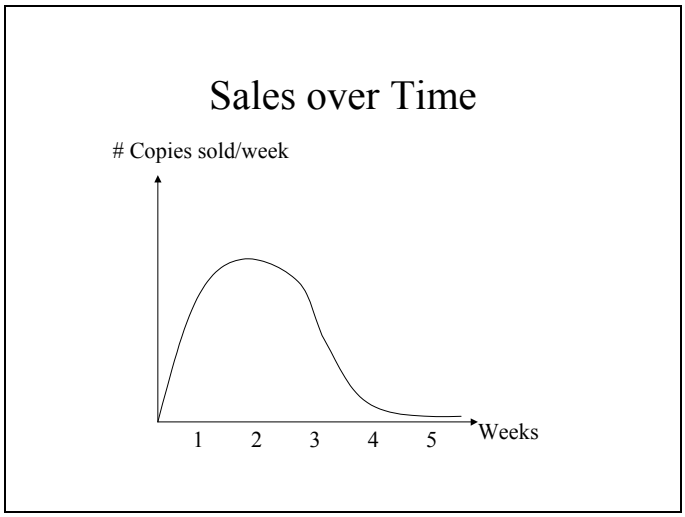

Fig 9 Possible sales curve

If we can but delay the copying and file-sharing for 4 weeks in this diagram, we would have saved the bulk of money that we stand making from the record in question. But there are two things that have to be established first, and that is a) if the sales curve looks like the one above and b) whether it will be possible to delay the stabilisation and noise dampening effects of the file-sharing network for the time necessary. Both these questions are very hard to answer.

The Madonna noise campaign consists of a large number of different files that are used in concert to create the noise effect. Not only one file has been used, but a cluster of decoys that make it truly hard to find the file in the file-sharing network.

Conclusions

Clearly, noise attacks are useful against the peer-to-peer networks, but they are most useful against the second generation of those networks. The first generation – Napster – was easy to attack since it had a central point of responsibility, so we can leave that generation behind. The third generation of semi-closed networks will not be open to these attacks as easily, since there is at least the possibility to qualify users before letting them enter the networks – any source of noise could then be quickly identified and disconnected.

Noise attacks are more suitable for the second generation peer-to-peer networks. These networks are inherently vulnerable to the quick dissemination of new music, and the contributory incentive mechanisms are slow enough so that the noise files actual acquire a certain dissemination rate before being eradicated by self-regulation deletion, rating and pure flow of authentic files.

These new types of attacks will come with complex legal problems, and the different legal aspects need to be thoroughly understood before Berman Laws are introduced and formulated, if, indeed, they should at all be formulated – arguably they are hard to enforce and monitor.

Opening the peer-to-peer networks to noise attacks and architectural self-defense might seem an intriguing and appealing way of destroying the wide-spread piracy in these networks, but there is a clear and present danger that this will backfire and cause users to flood legitimate systems or attack them in other ways to disrupt their functionality.

The answer to the machine is probably not in the noise, either.

References

Adar, E and Huberman, B "Free Riding on Gnutella" First Monday, volume 5, number 10 (October 2000) (http://firstmonday.org/issues/issue5_10/adar/index.html[2003-04-07])

Allan, S, Green, S, Friedman, J, Harrington, B and Johnson, L "New Technology and the Law of Copyright: Reprography and Computers" in Bush, George Technology and Copyright: Annotated Bibliography and Source Materials (Lomond Systems 1978) Originally in UCLA Law Review 15:993-1028 1968

Barlow, John Perry "The Economy of Ideas" Wired Mar 94.

Biegel, S Beyond Our Control: Confronting the Limits of Our Legal System in the Age of Cyberspace (MIT Press 2001).

Carey, Mark and Wall, David (2001) "MP3:The Beat Bytes Back", International Journal of Law, Computers & Technology, Vol 15, No.1 35-58,

Carroll, M (2002) "Disruptive Technology and Common Law Lawmaking: A Brief Analysis of A&M Records, Inc. v. Napster, Inc." Villanova Sports and Entertainment Law Journal, Vol. 9, No. 5, 2002.

Clark, C 'The Answer to the Machine is in the Machine', in: P. Bernt Hugenholtz (ed.), The Future of Copyright in a Digital Environment, The Hague: Kluwer Law International

Crews, C "One Internet Is Not Enough" TechKnowledge Issue #3 April 11, 2001 (http://www.cato.org/tech/tk/010411-tk.html82003-04-07])

Daswani, N and Garcia-Molina, H "Query-Flood DoS Attacks in Gnutella" Proceedings of the 9th ACM Conference on Computer and communications security 2002, November 18-22, Washington, DC, USA.

Freenet website(http://freenetproject.org/tiki-index.php?page=Philosophy[2003-04-10])

Jesdanun, A "Internet file-swapper frustrates entertainment industry" L.A. Daily News (http://www.dailynews.com/Stories/0,1413,200~20950~1151514,00.html[2003-04-07])

Kazaa website (http://www.kazaa.com [2003-04-10])

Lessig, Lawrence, Code and Other Laws in Cyberspace (Basic Books 1999)

Neo-Modus website (http://www.neo-modus.com/[2003-04-10])

Oram, Andy, (ed), Peer-to-peer : harnessing the benefits of a disruptive technology. Cambridge, MA: O'Reilly 2001.

Perritt, Henry H Jr "Mapping the Information Superhighway" in International Journal of Law and Information Technology Vol 3 no 3 Winter 1995 (pp 201-213) p 210)

Shannon, C "A Mathematical Theory of Communication" The Bell System Technical Journal, Vol. 27, pp. 379–423, 623–656, July, October, 1948.

Yen, A (2003) "A Preliminary Economic Analysis of Napster: Internet Technology,Copyright Liability, and the Possibility of Coasean Bargaining", University of Dayton Law Review (forthcoming),