

# From Arms Race to Mutual Cooperation – Towards Copyright Peace on the Internet?

*Mr. Ville OKSANEN, Mr. Mikko VÄLIMÄKI*

*Helsinki Institute for Information Technology (HIIT)*

*Software Business and Engineering institute (SoberIT)*

*P.O.Box 9800, FIN-02015 HUT, Finland*

Tel: +358 40 5368583; Fax: +358 9 6949768

[Ville.Oksanen@hiit.fi](mailto:Ville.Oksanen@hiit.fi) - [Mikko.Valimaki@hut.fi](mailto:Mikko.Valimaki@hut.fi)

It is often questioned why the content industry has started to wage lawsuits against consumers instead of making better and more affordable products. In this article, we try to first find reasons for the actual behavior of the content industry suggesting that the court strategy may be in fact more effective than it should be based on the pure likelihood of being sued. We also discuss various counter-measures the consumers have taken to minimize the risk of getting sued and compare the results to the popular “darknet” scenario proposed by Microsoft researchers.

Next, we take a look into the future by describing two opposite scenarios. In the first one we assume that digital rights management is omnipresent because all digital devices are required to have hardware support for government mandated trusted computing-platform. In the second one users are allowed to use whatever hardware available and “mobile mesh” is the prominent way to connect to the Internet. We also discuss the societal effects of the scenarios concentrating on the effects to general welfare and creativeness.

## Contents

<b>1. Introduction</b> .....	<b>2</b>
<b>2. Origins of Copyright Discussion on the Internet</b> .....	<b>3</b>
2.1 Early days.....	3
2.2 Case Scientology.....	7
<b>3. Content industry v. files sharers</b> .....	<b>10</b>
3.1 Background .....	10
3.2 Classical model .....	10
3.3 Corrected model.....	14
3.4 Darknet or the Barbed Wire Model.....	16
<b>4. Scenarios for the future</b> .....	<b>17</b>
4.1 Omnipresent DRM.....	17
4.2 Inside Mos Eisley.....	19
<b>5. Conclusion</b> .....	<b>20</b>

## 1. Introduction

The Internet has not treated the owners of copyrighted works well. The level of unauthorised copying has been staggering since the invention of the present-day peer-to-peer file sharing systems. However, the content industry does not show any signs of dying despite excessive copying. On the contrary, 2003 was very successful for the music industry in quite many countries including New Zealand, UK, Finland and the Netherlands.<sup>1</sup> Also the movie industry has been continuously breaking sales records during the last few years with rapidly increasing DVD sales and rentals.<sup>2</sup>

---

<sup>1</sup>Worldwide CD sales statistics can be found from <http://www.ifpi.org>

<sup>2</sup> At least in the US, DVDs present today well over 2/3 of the movie industry's annual sales and the share of DVD is still growing. See e.g. The Economist: Hollywood has learnt to love the DVD, but can it repel the pirates? February 5th 2004.

On this background, it is often questioned why the content industry has started to wage lawsuits against consumers instead of making better and more affordable products. In the first part of this article, we try to first find reasons for this behaviour and suggest that the court strategy may be in fact more effective than it should be based on the pure likelihood of being sued. We also discuss various counter-measures the consumers have taken to minimize the risk of getting sued and compare the results to the popular “darknet”-theorem proposed by Microsoft researchers.

In the second part of the article we take a look into the future by describing two opposite scenarios. In the first one we assume that digital rights management is omnipresent because all digital devices are required to have hardware support for government mandated trusted computing-platform. In the second one users are allowed to use whatever hardware available and “mobile mesh” is the prominent way to connect to the Internet.

In the last part of the article we consider possible incentive models for content creation in the previous scenarios. Especially, we debate the effectiveness of traditional copyright licensing compared to compulsory licenses and hardware levy schemes. We also discuss the societal effects of the scenarios concentrating on the effects to general welfare and creativeness.

Our method can be perhaps described as microeconomic anthropology. We refer extensively to Usenet postings and try to find out more realistic assumptions on how a primitive economy mainly consisting of “pirating” and “law-abiding” consumers functions.<sup>3</sup>

## **2. Origins of Copyright Discussion on the Internet**

### **2.1 Early days**

The discussions about possible copyright violations date back to the very early days of Internet. The earliest discussion about copyrights in the Usenet can be traced back to 1982. Most likely there has been even earlier discussions in different bulleting boards predating the birth of Usenet. The discussions retrieved from Usenet were also surprisingly similar compared to the one we have

---

<sup>3</sup> For discussion on methodology see Alf Rehn: *Electronic Potlatch: A Study on New Technologies and Primitive Economic Behaviors*. Stockholm: Royal Institute of Technology, 2001.

today. Only the scale was very different – for example term “copyright violation” was used only 59 times between May 1981 and May 1986.<sup>4</sup>

A striking example of this is a post made by Tim Maroney to the Net.General –newsgroup:

```
Message-ID: <bnews.unc.4367>
Newsgroups: net.general
X-Path: utzoo!decvax!duke!unc!tim
From: unc!tim
Date: Tue Dec 7 03:03:46 1982
Subject: Massive copyright violations on the net
X-Google-Info: Converted from the original B-News header
Posted: Mon Dec 6 09:25:41 1982
Received: Tue Dec 7 03:03:46 1982
```

It is very common for people who find some piece of prose pleasing to post it to the net. Most commonly, these are reviews of books, but I have seen entire essays and such posted. Although the motivations of the people who do this are admirable, it is past time for someone to point out the following:

This is a crime. It is a crime to publish or in any way reproduce for public consumption such copyrighted materials without explicit permission. It is also a crime to rebroadcast knowingly such materials. All sites which broadcast these are guilty.

This may seem like a minor crime, since no one is making any money from it. This is a false impression. Place yourself in the position of the writer who lives from day to day on the earnings of his or her writing. These people are not, like most net contributors, people who play around with writing, people who have a neat idea and casually decide to share it with people, but professional craftsmen. To infringe on their copyrights this way is to steal from them. If you have sufficient respect for the writer that you wish to share his or her work, then have enough respect not to steal from them. Many writers would probably not object to the posting if you asked, but please do ask. Write in care of the publisher, or get a phone number from the publisher (or the phone book). Show some consideration; suppose someone were to take a piece of your commercially distributed software and post it. Thank you for reading this.

Tim Maroney  
unc!tim

Tim’s post generated 14 replies to the Net.Followup. Most of these posts asked for more information or agreed with his position. Mark didn’t:

```
Message-ID: <bnews.cbosgd.2878>
Newsgroups: net.followup
X-Path: utzoo!decvax!harpo!npoiv!npois!cbosgd!mark
From: cbosgd!mark
Date: Sat Dec 11 03:34:00 1982
Subject: Re: Massive copyright violations on the net
References: <bnews.arizona.1267>
X-Google-Info: Converted from the original B-News header
Posted: Fri Dec 10 13:11:07 1982
Received: Sat Dec 11 03:34:00 1982
Reply-To: mark@cbosgd.UUCP (Mark Horton)
```

---

<sup>4</sup> Google’s Usenet Archive starts from May 12<sup>th</sup>, 1981

Look, you're getting it wrong. It may be a copyright violation to post copyrighted things on USENET, but there is no way you can sue the net (or an individual site) or bring down the net. That's like making the CB radio band illegal because somebody uses profanity on the air. It's like arresting your mailman because he delivered a letter whose contents are a threat to the life of the president.

The network as a whole is not responsible for assuring that the things posted to it are free and clear. Neither is a particular site. The person responsible (that's PERSON, you can't throw a machine in jail) is the one who posted it in the first place. S/he knew (or should have known) that by posting it, they are making 400 copies and distributing them to 10000 people. We should make people aware that they should not post copyrighted material without permission, but the network as a whole is not threatened.

Mark

So, basically the modern copyright discussion was more or less born in that thread. Tim's arguments and rhetoric is very similar like the one the content industry is using today. Mark made the same case as KaZaA et al have made later. Only typical user rights –comments with references to the fair use were missing from the thread. They did not really exist in other places either, most likely because most of the people just ignored the question. Even the landmark outcome from the Sony case was only celebrated in two short messages:

The life on Internet remained relatively calm during most of the eighties and early nineties. The biggest disputes pertained to software copyrights. The net was used as a distribution channel to unauthorized copies of different commercial software, which angered persons like future EFF co-founder Brad Templeton:

```
Relay-Version: version B 2.10 5/3/83; site utzoo.UUCP
Posting-Version: version B 2.10.1 6/24/83; site looking.UUCP
From: brad@looking.UUCP (Brad Templeton)
Newsgroups: net.followup,net.news,net.legal
Subject: Copyright Violations - how can software people do this
Message-ID: <140@looking.UUCP>
Date: Thu, 22-Mar-84 00:00:00 EST
Article-I.D.: looking.140
Posted: Thu Mar 22 00:00:00 1984
Date-Received: Thu, 22-Mar-84 04:21:47 EST
References: <778@nsc.UUCP>
Organization: Looking Glass Software, Waterloo, Ont
Lines: 46
```

I am amazed to see people on the net, most of whom work in software, actually defending copyright violators. Don't you have any interest in your own welfare?

Nobody know how much microcomputer software is stolen by people who "just copy it", but I would expect that conservatively one copy is stolen for each legitimate copy sold. Microcomputer software is a billion dollar industry (at least, probably more), so we are talking about probable billions in theft. Billions that were stolen from US.

If people paid for the software they steal, I know I would be a great deal richer and so would many of you. Either salaries would be higher or prices of software would be lower due to the increased volume.

We must work very hard to combat this attitude. As we enter the so-called "information age", information will become a very important form of property, and thieves will sap our money even more so than they do now. It applies to music, too. How many of you have played thief by taping a record just to save \$6 to \$10? I admit I used to, but haven't in many years.

The other day I met a kid (about 17) in a computer store:

Kid: You have a computer

Me: Yes, I have several (After all, it's how I make my living)

Kid: Do you have a Commodore 64?

Me: Yes, I have one of those

Kid: Got any games for it?

Me: I have written some games, yes.

Kid: Wanna trade?

Me: For what?

Kid: I have [some game]

Me: Did you write that?

Kid: No, I just got it.

Me: You mean you stole it?

Kid: No, I copied it. (And he really thought there was a difference)

Me: Is it for sale.

Kid: No. Well, in the stores I guess..

Me: So you are a thief.

Kid: Everybody does it...

Me: and that makes theft OK?

Kid: Everybody does it.

You've seen this kid yourself, I am sure, for he's everywhere. One little copy doesn't hurt the author, just like one little beer can doesn't ruin the park....

--

Brad Templeton - Waterloo, Ontario (519) 886-7304

The distribution of illegal material was mainly done via FTP-servers. Usenet did not have yet that active role in illegal distribution because binary attachments were frowned upon. This made the surveillance relatively easy for organizations like SPA and BSA, because the targets were centralized.<sup>5</sup> Of course, the limited user base did not hurt either. As a matter of fact, during the 80ties, the BBS (bulletin board system) was the distribution method of choice for most of the "warez-groups", because Internet-access was not generally available. Peer to peer – distribution was also widely used, but the carrier was bit more old fashioned i.e. the postal system. Also so-called copy-parties were common. In these events people get together (typically at some unsuspecting school e.g. under the pretence of "programming contest") to share their copied software.

Of course, the industry did not really exactly like the situation. Their response was multi-pronged. At the beginning they relied more on educating the users and used different copy protection schemes. After this was found to be ineffective and even counterproductive because copy

---

<sup>5</sup> Bronwyn Fryer: "The Software Police", Wired 3.05, <http://www.wired.com/wired/archive/3.05/police.html>

protections annoyed only users, which were using the legal versions of the software, they started to go after infringing (corporate) users and also attacked the sources of pirated software with help from the authorities.

For example, in Finland there were some very high profile cases against BBS-operators during the early nineties. These cases ended up to the highest court, which in the end lowered the fines considerably compared to the lower courts' decisions. Still, the public perception of very harsh penalties was born based on the early publicity of the cases. The practical effect was that the access to unauthorized material got much more limited. Still, a determined user could get practically any software package on the market "from a friend of a friend".<sup>6</sup>

## 2.2 Case Scientology

The first major copyright-fight pertaining to Internet was staged with this email:

```
From miscaviage@flag.sea.org Wed Jul 17 12:46:28 1991
Path: rpi!zaphod.mps.ohio-state.edu!think.com!snorkelwacker.mit.edu!ai-
lab!flag
!miscaviage
From: miscaviage@flag.sea.org (David Miscaviage)
Newsgroups: alt.religion.scientology.ctl
Subject: newgroup alt.religion.scientology
Message-ID: <80235@flag>
Date: 17 Jul 91 08:06:31 GMT
Control: newgroup alt.religion.scientology
Sender: news@ai.mit.edu
Lines: 0
Approved: miscaviage@flag.sea.org
```

With that message Scott Goehring created a new group "alt.religion.scientology" to Usenet. Following the Usenet tradition, the post was forged i.e. the sender's name was a misspelled version of the name of leader of Scientology.<sup>7</sup> What followed belongs to the legends of the Usenet.

The newsgroup did not draw much attention in the start. It was mostly used by two groups of people – by Scientology critics and by ex-members who still believed and followed the teachings but had left the organization. Only occasionally some low-level members participated to the debates. The posting activity remained quite low.

---

<sup>6</sup> This is based on the purely personal experiences

<sup>7</sup> Jim Lippard, Jeff Jacobsen, Scientology vs. Net, <http://www.skeptic.com/03.3.jl-jj-scientology.html#ars>, Goehring 's explanation: <http://tinyurl.com/3e8uw>

It took awhile for the management of Scientology to find the group but when it finally happened, they were less than pleased. The problem was that the “secret documents” of Scientology were often posted to the newsgroup and that caused a clear and present danger for their business model because the members were paying literally hundreds of thousands of dollars for that very same material. Also, the widespread knowledge about the key-beliefs and general conduct of the organization was likely to prevent or at least severely harm the recruitment of new members. The content of OT III-document illustrates rather well why this was the case (Appendix 1.)

In practice, Scientology did not have many other options than to try to prevent the dissemination of this information or to be gravely marginalized. To make their situation worse, the tools available at that time easily transferred the crucial information, which was mostly pure text. One could make the case that Scientology faced the quite similar problem as music industry is facing today with its business model.

Their solutions were also surprisingly familiar. They first tried to attack the communication channel i.e. delete the newsgroup. This backfired badly because it drew attention to otherwise rather obscure newsgroup without bringing any concrete results as most of the administrators ignored the RMgroup-notification.<sup>8</sup>

After they realized that the removal was not successful, the next step was attacking the postings. Usenet-protocol supports cancelling (and replacing) messages after they are posted. The first cancellations were done from real addresses but very soon they were replaced by anonymous forged messages. This approach gave some short term relieve but the critics counter-reacted and started to re-post the cancelled material. To make this easier, a program, which automatically posted a public notice of cancelled messages, was also created.

The technical solutions were more or less exhausted at this point. Scientology enlisted at that point their lawyers to the fight. They started to send warning letters to the people who were posting possible infringing material. Because this did not really bring any results, the decision to launch a full-scale legal attack was made. Scientology chose to target at the same time an end user (ex-scientologist Dennis Erlich), his Internet service provider (L.A. Valley College Bulletin Board

---

<sup>8</sup> <http://www.skeptic.com/03.3.jl-jj-scientology.html#attorneys>

System) and the up-stream provider (Netcom). This was the first time when an ISP was charged based on direct and indirect (vicarious) copyright violation. The outcome of the case was fortunate for the Internet. The judge cleared in *RTC v Netcom*<sup>9</sup> the Internet operators from liability of the acts committed by their customers. Also, the case against Dennis Erlich was later dropped.

Scientology started also an offensive against anonymous remailers. Some of the persons who were posting the “secret materials” had anticipated the possible legal risks and therefore had used these tools to hide their identity. The lawyers first sent letters asking the remailers to block posting to the alt.religion.scientology (a.r.s). Some of the remailers complied but most did not. Especially anon.penet.fi, the most famous remailer at that time, keep accepting posts to a.r.s.

On February 2, 1995, Juhan “Julf” Helsingius, the owner of anon.penet.fi, was contacted by Scientology informing him that his remailer had been used to publicly post information stolen from a private Scientology computer. The next day, Finnish police contacted Julf and demanded the information, and informed him that a warrant would be obtained if necessary. Julf did no budge. On February 8, Finnish police entered Julf’s home with a warrant granting them a right to seize his computers. To avoid the abrupt shutdown of his service, he had to give up the name, which the Finnish police passed on without delay to Scientology.<sup>10</sup> The case caused huge uproar in Internet and a.r.s become one of the most followed newsgroups in Usenet. The number of activists against Scientology soared.<sup>11</sup>

One of these people was Zenon Panoussis, a law school drop-out from Sweden. He created a surreptitious plan how to use Scientology’s aggressive legal strategy against them. He first posted openly their “secret documents” to Internet. As expected, Scientology sued him and forced the authorities to raid his home.<sup>12</sup> Zenon filed his defence to the court, which included the actual copies of his posts to Internet. Few days later, he asked for the copy of his own filing, which was now part of official court documents, took few copies of it, and submitted it to other Swedish authorities.<sup>13</sup> Here the catch was that Sweden had extremely strong publicity laws enforced by their

---

<sup>9</sup> L.A. Valley College Bulletin Board System was dropped out of the case

<sup>10</sup> He closed it down later anyway because he was no longer able to protect the identities of the posters

<sup>11</sup> <http://www.skeptic.com/03.3.jl-jj-scientology.html#penet>

<sup>12</sup> They did not found anything because Zenon had given the documents to his acquaintances and encrypted his hard drive with strong encryption.

<sup>13</sup> Rod Keller, Alt.religion.scientology Week in Review Volume 1, Issue 20 9/7/96, www.xenu.net

constitution.<sup>14</sup> After the documents were submitted to different governmental organizations, they were fully public and anyone could ask a copy of them for the cost of copying.<sup>15</sup> People also actually used the system and ordered countless legal copies of the “secret documents” e.g. from Swedish parliament’s library.

After Scientology found out that they couldn’t stop the discussion, they decided to start a “denial of service” –attack against a.r.s.<sup>16</sup> In practise they spammed the newsgroup with thousands of small email consisting of the same boilerplate introduction, a short quote from "What is Scientology" or some other official Scientology publication, and finishes with pointers to the official Scientology web sites. The fight did not end here, but it moved to other areas, especially to web and search engines, which are not anymore on the scope of this paper.

### **3. Content industry v. files sharers**

#### **3.1 Background**

The history of P2P-file sharing and related court cases has been covered extensively in countless papers.<sup>17</sup> In the first phase, content industry sued p2p software providers.<sup>18</sup> After the fight against software providers was lost, the industry did not have much options left. Suing individual users was more or less only option left.

#### **3.2 Classical model**

The traditional economic approach to calculate the effectiveness of the RIAA lawsuits would consider the utility of the file sharer. It can be calculated by reducing the costs of file sharing (the

---

<sup>14</sup> For example, the citizens may ask for the mail sent to the public authorities like the prime minister

<sup>15</sup> The story did not end here, there are much more bizarre twists like the later involvement of the US government

<sup>16</sup> There is only circumstantial evidence that Scientology is behind this. For example, Scientology was not interested to hunt down the persons behind this mass dissemination of their documents. More information: Frank Copeland, alt.religion.scientology Spam Attack!, <http://thingy.apana.org.au/%7Efc/scn/spam.html>

<sup>17</sup> Some more interesting takes offer e.g. Matthew Fagin, Frank Pasquale, Kim Weatherall, Beyond Napster: Using Antitrust Law To Advance And Enhance Online Music Distribution, 8 B.U. J. Sci. & Tech. L. 451, Jeremy Paul Sirota, Analog To Digital: Harnessing Peer Computing, Neil Weinstock Netanel, Impose A Noncommercial Use Levy To Allow Free Peer-To-Peer File Sharing, Harvard Journal of Law and Technology Fall, 2003

<sup>18</sup> In fact they went after Internet service providers in between before p2p technology became more widely used.

liability risk ( $C_l$ ), other costs like the price of broadband connection ( $C_e$ ) and the used time ( $C_t$ ) from the benefit (money saved by downloading the music ( $S_m$ )). The person uses file sharing software if  $S_m - (C_l + C_e + C_t) > 0$ .

The liability risk is usually calculated by dividing the number of filed court cases by the number of file sharers and multiplying that probability by the estimated fine, i.e.  $C_l = (N_{\text{cases}} / N_{\text{sharers}}) * C_{\text{fine}}$ . The problem with this approach is that it looks backwards instead of estimating the risk in the future. The reason is simple,  $N_{\text{cases}}$  should actually be  $N_{\text{new cases}}$ .

In this simplified model RIAA has a direct control of two variables, the number of (new) court cases and the price of the music ( $N_{\text{cases}}$  and  $S_m$ ). The estimated fine is mostly derived from the legislation but - if publicised as the case has been - the early out-of-court settlements form the base level for the calculation.

This approach is not so out of touch with the reality. Calculations like this are quite common in the Slashdot:

```
Re:Overall total? (Score:2)
by AstroDrabb (534369) * on 23-06-04 5:09 (#9502458)
```

```
Those who continue to do this are probably going to eventually get caught
```

```
The RIAA has sued about 3,429 people. There are _atleast_ 10,000,000 people in the USA alone that are using some type of file sharing (and that is not counting the rest of the world). so (3,429 / 10,000,000 = 0.0003429) * 100 = 0.03429. So you have a .03 percent chance of being caught by the RIAA. I don't think the RIAA has the "leg up" in this situation.
Senior Programmer
Davenport, FL USA
```

As a matter of fact, most of the discussions about RIAA's court filings included at least one of this kind of calculation.<sup>19</sup> The published figure about the average settlement (~3000\$) is also added often to these calculations. Thus, the outcome is that a person is better off practically always by participating in file sharing.

The simplified model does not take into account that  $C_l$  is different for different users. This is actually the only variable, to which the users have direct control.

---

<sup>19</sup> Another, more detailed example can be found from here:

<http://yro.slashdot.org/comments.pl?sid=105737&cid=9002536>

Based on the discussions, there seems to be four typically suggested to lower the risk. First of all, the users may choose to limit the number of shared files. RIAA has been pointing out that it is targeting mostly users who have more than 1000 songs in their shared folder and thus sharing less lowers the likelihood to be sued:

On Monday, September 8th, the RIAA, on behalf of its member companies, filed the 261 copyright infringement lawsuits against individuals who were illegally distributing, on average, more than 1,000 music files for millions of other peer-to-peer network users to copy for free.<sup>20</sup>

This strategy is of course beneficial to RIAA's goals because it rises  $C_t$  due to lower number of available sources. Targeting big sharers makes the cases also appear less aggressive. Of course, there are certain risks for RIAA in this strategy:

zigging when they should zag (Score:3, Insightful)  
by Anonymous Coward on 25-06-03 21:40 (#6295717)

Well, these clowns have been fighting the wrong battles here for ages. This one is no surprise.

The strength of P2P has nothing to do with the small % of users who share huge amounts of material. It's the combination of thousands of individuals each sharing a small amount of material. Seeing tactics like this is even counterproductive because it sends the message that sharing a few files is okay; the real crime is sharing lots of files.

Even with its size, the RIAA isn't big enough to sue the litte guys who are the engine of P2P. This human-redundancy is why P2P is around to stay.

Still, it is good to notice that this works to other direction, too. If a large number of P2P-users decide not to share *any* files - i.e. leach - the  $C_t$  rises sharply. This may turn the utility negative for some of the users, which means that  $N_{users}$  will decrease. This raises the likelihood to be sued thus the utility drops even further. This kind of "positive" feedback loop is of the few realistic options, which have real effect curbing the file sharing.

Second way to lower risk is quite close the first one: instead of sharing fewer songs, a person chooses to share only few or none "hot" songs. This approach was relatively popular in the beginning of the lawsuits because the early subpoenas contained the names of the infringing files and from that information it was obvious that some artists very monitored more closely than others.

---

<sup>20</sup> RIAA Press Release: 64 Individuals Agree To Settlements In Copyright Infringement Cases, 29.9.2003.

<http://www.riaa.com/news/newsletter/092903.asp>

The third option is to try to limit the access of RIAA to the shared files. The simplest form of this is turning off the “show all shared files” option. The more advanced option is to use specific lists of blocked addresses. Some P2P-software has this ability built-in (e.g. Emule) but it is also possible to use specific program for this purpose like Peer Guardian<sup>21</sup>, which acts like a firewall and prevents all connections from blocked addresses. In addition, some firewalls support blacklisting.<sup>22</sup> The bad news for RIAA is that this approach lowers  $C_1$  without having significant effect to  $C_t$ .

The good news with this approach is that RIAA (and companies which sell monitoring services) can very easily check whether their IP-addresses are blocked or not and in latter case just to change to a new IP-address(range). The blacklists have to be publicly available to be useful for normal users and therefore the content industry has unavoidably the upper hand in technology race.

The last and potentially the most worrisome option for RIAA is avoiding lawsuits by moving to more safe P2P-networks. In the beginning this movement was mostly from KaZaA to different Edonkey-clients and to Bit-Torrent. Neither of these two programs offer any advanced privacy protections and thus the benefit came from the fact that RIAA was most worried about the biggest network. After the usage of Edonkey and Bit-torrent rised, the networks started to draw attention and thus the early benefits were lost. The next step will be more anonymous networks like Freenet and Mute. The problem with these networks is that they are very hard and slow to use and hence  $C_t$  is very high. Alienw’s experiences demonstrate this:

```
Re:Protect your privacy (Score:2)
by alienw (585907) on 29-04-04 6:00 (#9003908)
MUTE is a piece of shit made by a complete idiot. Have you even tried using
it? My top speed on it was 500 BYTES per second. The retard who programmed
it used a text-based protocol that wastes an incredible amount of usable
bandwidth (and there isn't that much to begin with because the protocol is
inefficient). In short: good idea, incredibly bad implementation.
If you think this post needs to be modded down, try using the reply button
instead.23
```

Lastly, RIAA has been using one additional strategy to rise  $C_t$ . The networks have been poisoned with fake files, which typically have five seconds of real material in the start and the rest is some kind of annoying noise. P2P-networks have countered this attack by adding flagging possibilities for faked files and also by creating databases of faked files. The blocking lists typically protect

---

<sup>21</sup> <http://www.methlabs.org/methlabs.htm>

<sup>22</sup> More info: <http://methlabs.org/forums/forumdisplay.php?f=6>

<sup>23</sup> <http://yro.slashdot.org/comments.pl?sid=105737&cid=9001566>

against known sources of faked files. Thus this attack has been only successful insofar the users are technically unsophisticated, which is still quite acceptable from RIAA's perspective.<sup>24</sup>

### 3.3 Corrected model

The classical model would imply that RIAA is facing in practice an impossible task with its lawsuits. The strategy becomes more understandable after the model is redefined by using the theories behind behavioural (law and) economics.

In traditional model we used the following parameters

- The likelihood of penalty
- The size of penalty
- The benefits arising from the violation

We argue that the following parameters should be also taken into consideration:

- The reputational cost of violation
- The reputational benefit of violation<sup>25</sup>

In the current environment, the copyright violation is not generally speaking considered to be a serious crime. On the contrary, copyright is often seen just as tool for corporate suppression, which violation is more a civic duty than a crime. The post from Slashdot illustrates this position quite nicely:

```
Wow, we're on a roll today! (Score:3, Funny)
by DroopyStonx (683090) on 29-04-04 1:24 (#9001875)
```

```
An interview with fuckwad Valenti, and now more RIAA lawsuits! Woweee!
```

```
They're sure doing a good job into scaring me... scaring me so much that
tonight, I'm gonna be downloading more than normal!
```

```
Got Movies? [newzbin.com]
Got Music? [newzbin.com]
```

---

<sup>24</sup> According to a recent study, many Kazaa users don't know when they share files. See Nathaniel S. Good and Aaron Krekelberk: Usability and privacy: a study of Kazaa P2P file-sharing, 2002. Available at [www.hpl.hp.com/shl/papers/kazaa/KazaaUsability.pdf](http://www.hpl.hp.com/shl/papers/kazaa/KazaaUsability.pdf)

<sup>25</sup> Cass Sunstein, Why societies need dissent, 2003, .p 46

I do NOW, and so can you! Aim your middle fingers at them and grin, because this is the best weapon against 'em.

That said, there are a small but vocal minority of people, who truly believe that file sharing is stealing. Their posts are commonly moderated down and other posters also quite often “flame” these people. RIAA’s lawsuit may never the less strengthen their position. At least RIAA claims that this is the case:

New consumer survey results from a November poll, among 802 Americans age 10 and over, show that 64 percent of those polled understand it's illegal to "make music from the computer available for others to download for free over the Internet." That's up from 37 percent in November 2002, and for certain subgroups, the new awareness numbers are even higher -- for example, 69 versus 16 percent among "regular Internet users."<sup>26</sup>

In other words, the law suits seem to be at least partly effective way the strengthen the perception that file sharing is wrong.

Other behavioural effects may also add up to the outcome. For example, people tend to be conformists i.e. they prefer to follow other people’s behaviour.<sup>27</sup> If RIAA can make a credible case, that vast numbers of people have stopped using P2P-networks, this could actually be more effective than to make a point that file sharing is illegal. Indeed, this theme has been in prominent role in RIAA’s press releases. Unfortunately, it has been effectively oppugned by independent research groups.<sup>28</sup>

Another example of behavioural effects in the play here is most likely *availability heuristic*.<sup>29</sup> People tend to overestimate the likelihood of events, which has been recently visibly in the news. For example, people typically overestimate the risk to die in a plane accident. This works also to the other direction, which means that people underestimate the risk arising from frequent events like car accidents. This means that RIAA will maximize the result of its lawsuits by keeping them as much

---

<sup>26</sup> RIAA Press release: Music Industry Commences New Wave of Legal Action Against Illegal File Sharers, 3.12.2003, <http://www.riaa.com/news/newsletter/120303.asp>

<sup>27</sup> See Sunstein pp 48-51.

<sup>28</sup> Big Champaign’s Eric Garland’s (CEO) presentation at Computer, Freedom & Privace 2004 is a very good example of this: [http://www.cmcgc.com/cfp2004/422\\_Plenary\\_8.mp3](http://www.cmcgc.com/cfp2004/422_Plenary_8.mp3)

<sup>29</sup> Sunstein pp 91-93.

as possible in the news. In this sense even the cases against innocent grandmothers and 12 year-old schoolgirls are beneficial, because they strengthen the perception that nobody is in safe.<sup>30</sup>

### **3.4 Darknet or the Barbed Wire Model**

A final model assumes that copyright violators can be separated and the business focus can be put on the well-behaving consumers. This model can be attributed to Microsoft researchers arguably in charge of the company's trusted computing initiative who wrote in a seminal paper on "darknet" as follows:<sup>31</sup>

There is evidence that the darknet will continue to exist and provide low cost, high-quality service to a large group of consumers. This means that in many markets, the darknet will be a competitor to legal commerce. From the point of view of economic theory, this has profound implications for business strategy: for example, increased security may act as a disincentive to legal commerce.

As an answer, the paper suggests that in the future "PC's are Rendering Devices through mandated watermark detection" who "eliminate objects that originated in the darknet". This is exactly the strategy Microsoft has taken in its trusted computing initiative. One could also describe it as a kind of barbed wire approach that would classify all unauthorized content as "dark" and in the long term unusable on the trusted (and legal) computers. Interestingly enough, despite its name, darknet seem to be the liberal network between the two with consumer pressure towards it. Instead of making content more secure, the approach aims to make computer use in general more controllable. The Darknet approach also disregards the value of legal actions by content owners. Paradoxically, the premises of the approach (secure hardware) are built on the same deterministic premises (secure software) it tries to oppose.

---

<sup>30</sup> The theory behind availability heuristic is not universally endorsed. For example, Gregory Mitchell criticizes its premises in his article "Taking Behavioralism Too Seriously? The Unwarranted Pessimism Of The New Behavioral Analysis Of Law", 43 Wm. & Mary L. Rev. 1907, 2002.

<sup>31</sup> Peter Biddle, Paul England, Marcus Peinado and Bryan Willman: The Darknet and the Future of Content Distribution, Microsoft Corporation, 2001. Widely available on the Internet.

## 4. Scenarios for the future<sup>32</sup>

Predicting the future is anything but an easy task. One of the often-used tools to help on this process is a scenario-based approach. The scenario-based approach can be categorized into 20 different methods.<sup>33</sup> In this paper we use a very basic solution, in which we describe the two extreme visions for the future. The idea here is to pinpoint the possible major driving forces behind changes and consider what kind of results they could cause. The optimal number of different scenarios is typically five or more, but in this case we believe that more is actually less. The created scenarios will hopefully demonstrate the best outcome really is in the middle and not in the extremes.<sup>34</sup>

### 4.1 Omnipresent DRM

Trinity's morning did not start well. A RIAA SWAT-team storming into the house is not the best possible way to wake up. Before Trinity could rise up from the bed, she was already handcuffed.

“What's going on, I haven't done anything wrong”, she screamed.

The leader of the SWAT-team responded calmly: “You have been charged based on unauthorized public performance of a copyrighted material. Resistance is futile and will lead to additional charges.”

“What!”

“Yeah. Two days ago you arranged a birthday party to your daughter. There were more than 12 guests and you did not get a license for singing ‘Happy Birthday’. One of the children turned you in to get lower sentence for file sharing.”

“You must be kidding!”

“No, one year ago the new “Zero Tolerance for Copyright Theft” -act was enacted. Now all copyright violations are punishable by mandatory prison sentences. Also, RIAA has now full law enforcement rights in criminal cases. You should have heard about this by now, the TV has been full of advertisements about the War on Copyright Theft”

---

<sup>32</sup> The authors of this paper readily admit, that this section is not so scientific, but it was very fun to write and it would be shame to remove it from the paper.

<sup>33</sup> Max Moore, Grasping the Future: Comparing Scenarios to

Other Techniques, 2001, <http://www.kurzweilai.net/meme/frame.html?main=/articles/art0178.html>

“But I don’t have a TV!”

“Too bad.”

Trinity was escorted to a black van, which was waiting outside. A social worker had already come to the house and was preparing to take her daughter to a governmental re-education camp. The neighbours were shocked to find out that a copyright thief had been living in their quiet neighbourhood. The van headed for the closest prison.

“Ok, ETA 15 minutes to the gate. We have one gue... WHA...” <craczzshhhhhhhhhhhhhhh>

The transmission was abruptly terminated.

Trinity’s life was about to take another bizarre turn. The van was attacked by Copy Fighters’ Front (CFF), a movement, which had started in the academia during the last decade of the past millennium, but had later turned into militant guerrilla organization opposing copyright and digital rights management. The group’s leader was John C, a charismatic open source activist, who had excellent knowledge on armed fighting. RIAA’s forces did not have a chance against fierce attack and Trinity was quickly freed and transferred to another, unmarked van, which headed towards sea.

Trinity was moved to a heavily armed ship, which was waiting in the international waters. She was told that the next stop would be Mos Eisley. To her great relief, her daughter was also bit later brought to the ship.

“So, could somebody to finally explain what is going on?” she finally asked on the third day on the sea.

One of the CFF’s fighters started to explain:” The content industry used to claim that ‘piracy’ supports terrorism. That was of course just rhetoric from their part, but unfortunately the real terrorist got the point and started really attack against intellectual property held by US companies. They also used the gained money to finance real attacks inside the United States. After the evidence of this was published, the public mood changed radically against any copyright violations. The content industry did not need to ask new rights, they were given to them without any real opposition or debate. Mandatory digital rights management for all computers was the first move, which was

---

<sup>34</sup> This is also the main argument of Lawrence Lessig, see e.g. Lawrence Lessig, Free Culture, 2004, The Penguin Press

quickly followed by another steps like a duty to register all devices, which are used to make or store software, music or videos. Open source became obsolete, because the developers could not run the software because of the trusted computing.”

“Yeah, now you mentioned it, I remember hearing something like that... But I didn’t think at that time that it would have been such a big deal” Trinity sighted

“Your were not alone. And of course, these moves did not totally end the unauthorized copying. The politicians responded to the situation by adding harsher and harsher penalties. Also, the questioning the sensibility of the system was made illegal by framing it as “aiding piracy and terrorism”. We did not have any other options to go underground and start real fighting.”

## **4.2 Inside Mos Eisley**

The ship stopped at the front of Mos Eisley Cantina. Mos Eisley had become the new safe heaven for people who believed that all intellectual property rights are wrong. The country had fought against new international IPR-treaties with no avail and in the end it was kicked out of the world trade system because it refused to comply with the new regulations. As a result the economic situation of the country was now slowly deteriorating in lack of foreign investments.

The country has adapted the compulsory levy model pushed notably forward by Electronic Frontier Foundation and some academics like professors William Fisher.<sup>35</sup> The problem was that less and less money was coming into the system because of the worsening economic conditions. The amount and allocation of collected levies was a constant sore point in Mos Eisley politics. Many artists were forced to get a normal day job to finance their life.

The government had also forbid selling proprietary software. In the start it worked well, but after the governmental funding for free software projects ended, the development slowed down badly because the service market inside Mos Eisley was not big enough to sustain the development. Of

---

<sup>35</sup> See Fisher, William: Promises to Keep: Technology, Law and the Future of Entertainment. Stanford University Press, forthcoming 2004 and EFF: Making P2P Legal, available at <http://www.eff.org/share/legal.php>

course it did not help that the rest of the world was using systems based on trusted computing, which were not compatible with free software.

Still, there were also some very positive sides. The worsening situation in the US had caused projects like Internet Archive to depart to Mos Eisley. As a result, Mos Eisley had become the safe heaven for the world's cultural heritage. The non-existing copyright had made it possible to digitise the all existing works and thus the library of Alexandria was recreated. The library material was not only stored in a centralized servers but people were free to store, edit and share with their personal devices. Modern, naturally freely available, software tools had made this also so easy that people could participate to the re-creation without any previous training.

## **5. Conclusion**

We have now looked into the past, present and future of copyright issues on the Internet. From the history it is easy to see that nothing is really new. Only the scale and scope have changed. Secondly the Scientology case clearly demonstrated that after the information has once been digitised and released to the Internet, it's impossible to get the "genie back to the bottle". The more aggressive methods are used to stop the distribution, the stronger is the resistance.

Recording industry's current chances in the fight against file sharing do not look very good. The sheer numbers favour very strongly the file sharers. Still, the lawsuits may actually be more effective than what they really should be because of the behavioural economic aspects. Recording industry seems to have taken this into consideration in its campaign and it presses right themes, which most likely will resonate with people's opinions about file sharing.

The last part should have few teachings. Maximizing the protection will inevitably cause collateral damage to the society. For example, the tools, which are used to make and store music, allow typically the production of pirated songs and thus in "DRMtarian" society the access to them has to be strictly controlled, which has serious negative effects to the cultural production. In other hand, minimizing the protection will harm production of the cultural goods, but it will be bring other, mostly cultural benefits. The free and easy access to all human knowledge ever created could truly foster the humankind.

## Appendix 1. OT III

The head of the Galactic  
Confederation (76 planets around  
larger stars visible from here)  
(founded 95,000,000 yrs ago, very space opera)  
solved overpopulation (250 billion  
or so per planet -- 178 billion on  
average) by mass implanting.  
He caused people to be brought to  
Teegeeeack (Earth) and put an H Bomb  
on the principal volcanoes (Incident 2)  
and then the Pacific area ones  
were taken in boxes to Hawaii  
and the Atlantic Area ones to  
Las Palmas and there "packaged."  
His name was Xenu. He used  
renegades. Various misleading  
data by means of circuits etc.  
was placed in the implants.  
When through with his crime Loyal Officers  
(to the people) captured him  
after 6 years of battle  
and put him in an electronic  
mountain trap where he still  
is. "They" are gone. The place (Confed.)  
has since been a desert.<sup>36</sup>

Source: David S. Touretzky's OT III Scholarship Page, <http://www-2.cs.cmu.edu/~dst/OTIII/>

---