STS.085 Project Better title

Michael E Plasmeier <theplaz@mit.edu>

Stephen J Suen <ssuen@mit.edu>

Contents

[Exec Summary 3](#_Toc342831936)

[Problem Statement/Intro 4](#_Toc342831937)

[Evaluative framework 4](#_Toc342831938)

[Is if effective in reducing copyright infringement? 4](#_Toc342831939)

[Ease of Circumvention 5](#_Toc342831940)

[Economic 7](#_Toc342831941)

[Costs 7](#_Toc342831942)

[Artists 10](#_Toc342831943)

[Employment 10](#_Toc342831944)

[Technical 11](#_Toc342831945)

[Internet Infrastructure 11](#_Toc342831946)

[How in infringement detected today? 12](#_Toc342831947)

[Minimally necessary 13](#_Toc342831948)

[Non-infringing use 13](#_Toc342831949)

[DRM 15](#_Toc342831950)

[Fair Use 15](#_Toc342831951)

[Stakeholders 18](#_Toc342831952)

[Responsibility of Implementation 18](#_Toc342831953)

[*Proper Authority/Jurisdiction* 19](#_Toc342831954)

[*Financial Burden* 19](#_Toc342831955)

[Possible Political Resistance 19](#_Toc342831956)

[Synthesis 19](#_Toc342831957)

[Meta-analysis of Framework 20](#_Toc342831958)

[Current Policy Debates 20](#_Toc342831959)

[HADOPI (Stephen) 20](#_Toc342831960)

[6 Strikes vs Lawsuit – Plaz 21](#_Toc342831961)

[Description 21](#_Toc342831962)

[Analysis 23](#_Toc342831963)

[Upcoming policy debates 28](#_Toc342831964)

[Specific Policy Recommendation 28](#_Toc342831965)

[Other 28](#_Toc342831966)

[Share of work 28](#_Toc342831967)

[Cut Sections 28](#_Toc342831968)

# Exec Summary

TBD Currently proposal with minor edits

Our project aims to develop a framework for the cost-benefit analysis of anti-copyright infringement mechanisms.

* Will the policy actually make a difference?
* Can the policy be implemented robustly?
* Can pirates easily avoid the mechanism?
* What are the costs and challenges of implementation?
* Does the policy violate the standards of the Internet?
* Will the policy prevent us from accomplishing other goals, such as tightening up cyber security?
* Will certain actors incur a cost, and if so, who will pay for it?

Based on these issues, the long-term goal for this evaluative framework will be to encompass a common set of values, standards, and metrics for the analysis and discussion of future proposed anti-copyright infringement mechanisms. With this model, we hope to enable a more robust discussion of how to address the copyright infringement problem without compromising the underlying structures of the open Internet and—by extension—the civil liberties guaranteed by those structures and the ecosystem for innovation that they have enabled. This analysis will also take into account pragmatic issues of economic costs, possible political challenges, and other barriers to comprehensive implementation. We will also be sure to examine copyright law pre- and post- Internet, to see how notions of intellectual property and proper enforcement of those exclusive rights have changed over time, in order to better contextualize the issue.

To illustrate the usefulness of such a framework, we will show it in action by running an analysis of recent graduated response policies proposed to combat online copyright infringement—specifically, the HADOPI law in France and the “six strikes” Copyright Alert System being implemented here in the US as part of an agreement between the MPAA, the RIAA, and a number of major ISPs. To put this assessment into perspective, we will also use our framework to evaluate the effectiveness of the previous anti-copyright infringement paradigm of filing lawsuits against individual users, using it as a benchmark for comparison. Through this analysis, we will be able to identify the merits and downsides of graduated response mechanisms, discuss them in relation to traditional copyright litigation strategies, and provide comprehensive policy suggestions.

# Problem Statement/Intro

## Copyright

*Copyright* is a legal concept in which the government grants the creator of an original work exclusive right to the work. It is a form of *intellectual property*, a category which includes patents, trademarks, and trade secrets, all of which are *intangible assets*. Governments want to encourage the creation of “works of the mind” by giving the original creators exclusive rights for a period of time. A copyright holder is granted certain *exclusive rights* to a work, such as the rights to reproduce, distribute, display, or perform the copyrighted work, or to make derivative works. In the United States since 1989, content is automatically copyrighted when it is reduced to tangible form (ie. written down).

## Copyright Infringement

*Copyright Infringement* is the unauthorized use of works under copyright, for example, making a copy when one is not authorized to do so. For example, if one were to make a copy of the latest Taylor Swift CD one purchased at Walmart and give it to a friend, that would be copyright infringement. Copyright infringement is often referred to *copyright infringement*.

Copyright infringement has been and continues to be a big problem for the creative content industries, as technology that made copies, particularly digital technology, has become more accessible to consumers. The Internet has only exacerbated the problem, as the Internet allows one to send files across the globe with varying degrees of traceability.

While estimates on the scale of the problem vary, most people believe something should be done to reduce the availability of unauthorized copies of work. Should something be done?

Estimate scale of the problem

For the last decade, the content industries have been trying to fight unauthorized sharing over the Internet. A number of methods have been tried, including having the industry sue individual downloaders. However, recent efforts have been coalescing around so called “graduated response” efforts. Under a graduated response system, a user is sent a number of warnings, before a penalty, which might include service termination. Such systems can be mandated by law, such as in France, or through a voluntary agreement with Internet Service Providers (ISPs) as in the United States.

# Evaluative framework

We attempt to establish a framework to evaluate proposals to combat copyright infringement.

1. Is effective in reducing copyright infringement?
   1. Ease of circumvention
2. Does it make economic sense?
   1. Revenue in reclaimed sales
   2. Positive effects on employment
3. Has minimal negative repercussions on internet
   1. e.g. DNS
4. Is it the minimum necessary?
   1. Non-infringing use of technology – effects on innovation (e.g. Megaupload, torrents)
   2. Fair use arguments (creative/cultural)
   3. Beneficial services
5. Will be acceptable to stakeholders (political/legal argument)
   1. Who will implement? Legal authority/precedents?
   2. Costs of implementation/enforcement
   3. Political views/possible challenges of stakeholders, e.g. industry, citizens, artists

## Is if effective in reducing copyright infringement?

1. Is effective in reducing copyright infringement
2. Ease of circumvention

The first question to ask about any policy is “is the policy effective in reducing copyright infringement?” A policy that does not reduce copyright infringement should not be considered further.

### Ease of Circumvention

A policy does not need to be ironclad in order to reduce copyright infringement. As an example, one does not need to look further than Section 1201 of the Digital Millennium Copyright Act. This section prohibits the circumvention of access control measures. Because of this section, it is illegal to make copies of DVDs. However, it is not illegal to make copies of CDs.[[1]](#footnote-2) Because of this, legitimate programs such as iTunes and Windows Media Player offer users the ability to make copies of CDs, but not DVDs.

It is certainly possible to download a program from the internet to make copies of DVDs, but the very fact that it is not easy prevents vast amounts of Americans from even trying.

It is not even that hard to find out how to do it. Searching for “how to rip a DVD” yielded instructions on the first result. Now such instructions are somewhat complicated, with instructions to download a .dll to a certain programs folder location, but it still requires moderate tech skills.

Keeping material illegal makes it harder to find. Even though the industry has been unsuccessful in shutting down the Pirate Bay, it has prevented it from becoming a legitimate business. By keeping the business illegal and keeping it on the run, the industry has made the life of the Pirate Bay harder.

However there is still a core group of techies and dedicated other folks who have the knowledge to learn how to circumvent these measures and cover their tracks.

(move below elsewhere?)

#### DNS Filtering

This can hamper the effectiveness of certain proposals. For example, SOPA proposed altering DNS information to remove sites that infringed on copyright.[[2]](#footnote-3) However, a user could just enter the IP address of a site instead.

DNS is a service of the Internet which maps friendly names such as “google.com” into IP addresses such as “74.125.224.35”. Each server[[3]](#footnote-4) on the internet has as IP address which is the way that other computers can route traffic to the server. DNS provides this mapping of IP. For example, thepiratebay.se is located at 194.71.107.15.

However, instead of entering the domain name into ones browser, one can enter the IP address of the server directly into one’s browser. This would allow the users to connect to the server, while bypassing the DNS service.

|  |  |
| --- | --- |
| Domain Name | IP Address |
| thepiratebay.se | 194.71.107.15 |

If the Pirate Bay ever has to change server hosts, then moving their IP address would be almost impossible, as these are assigned in blocks. For example, when the internet was first created large organizations such as MIT were given large blocks of IP addresses. For example, MIT has all of the IP addresses starting with 18. Servers then through Border Gateway Protocol (BGP) have rules to forward all traffic destined for IP addresses starting with 18 towards MIT since MIT is an “Autonomous System.” The same applies to Internet Service Providers or Hosting Providers. If the Pirate Bay changed hosting providers, their IP address would change. Under DNS, the Pirate Bay can slowly phase in their new IP address transparently.

This may be a significant factor. One study of spam messages showed that only XX% of messages contained an IP address instead of a domain name.[[4]](#footnote-5)

However, if their IP address was publically known, they would have to disseminate their new IP address, for example by posting it in Twitter or in a newspaper ad. There are even more subtle ways to do this on the Internet. Persons not in the United States could operate “darknet” DNSes. These DNSes would have addresses that the US had blocked[[5]](#footnote-6).

The United States government would have to be super careful about how it distributes the blacklist. If it was just a simple list that was public, then some people would just feed this list into their DNS system to allow users to continue to reach all of their old content. In addition, this list of copyright infringing sites would tell copyright thieves exactly where to look!

They could even be distributed, much in the way of BitTorrent itself is. For example, BitTorrent Distributed Hash Tables (DHT) work by giving each node a copy of the table or part of the table. A node then asks other nodes to share their tables. That way there is no one authoritative owner which would frustrate any attempt to take it down, because almost every node would need to be taken offline to bring it down.

(should these details be elsewhere?; really got into the weeds here; but where else would be best for this?)

This raises an interesting question: is it illegal to know the phone number of an illegal service? For example, say someone had the phone number of a drug operation. Is that in and of itself illegal?[[6]](#footnote-7) No, it’s only evidence that corroborates a story and could provide extra evidence against a person in court. By itself it is not illegal. Then how are knowing IP addresses any different? DNS is just a mapping of a name to a number. That should not in and of itself be illegal.

Multiple sites can live at the same IP address, through a technology called “vhosts.” Each server has only one IP address, but it can host multiple sites running on multiple domain names. Low-grade shared hosting often is set up in this way. If one were to ban an entire IP address, one could ban sites other than the one that was planned. The other sites running on the same server could be run by completely different entities who have no clue or control over the behavior of the other site. This is like shutting down the entire mall because one store is selling counterfeit handbags.

#### Digital Rights Management

To prevent misuse of copyrighted work, the content industries introduced *digital rights management*. DRM is used to prevent the copying or other unauthorized work of a digital work. DRM is controversial because it limits fair use rights and limits what legitimate customers can do with their purchases. DRM is often based on encryption.

However, at its core DRM faces a fundamental problem which limits its theoretical efficacy. A device must be able to play a particular work (for example a song) for the user to be able to listen to it. Society has developed encryption to protect two files from listeners in the middle as they cross a network. However, it is theoretically impossible to protect content which has to be decrypted and outputted on a device where the “advisory” (in cryptography terms) owns the hardware and has complete control over the hardware.

Thus DRM has been effective in limiting what honest and unsophisticated consumers can do with their work, but has done little to limit the availability of copying to sophisticated users. CDs are still sold without DRM, so it did little to matter that iTunes added DRM, except to only allow consumers to play their music on iPods. The illegally obtained material was not only free, but came without strings attached to it!

## Economic

1. Does it make economic sense
   1. Revenue in reclaimed sales
   2. Positive effects on employment

### Costs

Next, one should look at the costs of a policy to evaluate whether the benefits of the policy outweigh the costs of the policy. In addition, who bears the costs? The content industry? The government? Internet service providers?

#### How much does the government spend on anti-copyright infringement?

Find current costs spent on enforcement

http://arstechnica.com/tech-policy/2011/08/protect-ip-act-would-cost-taxpayers-47-million-private-sector-much-more/

For example, the Prioritizing Resources and Organization for Intellectual Property Act of 2008 (H.R. 4279) was estimated by the Congressional Budget Office to cost an additional $425 million dollars over 4 years by hiring a Intellectual Property Enforcement Representative in the Office of the President at $30 million per year, 10 intellectual property attachés to serve in United States embassies or other diplomatic missions for $21 million a year, and $64 million in additional funding for the FBI. [[7]](#footnote-8) There are already 8 attachés in Brazil, China, Egypt, India, Russia, and Thailand.[[8]](#footnote-9) The CBO budgets about $1 million dollars per agent for 4 years of service. Additionally the CBO predicts no substantial impact from increasing damages or asset forfeitures for the Crime Victims Fund or the Assets Forfeiture Fund. Additionally, the ﻿Title III would allow the Office of the United States Intellectual Property Enforcement Representative would be allowed to accept gifts, but the CBO does not predict much of an impact from this.[[9]](#footnote-10)

Too much of the wrong type of detail

#### How much is lost by copyright infringement?

Global recorded music sales have plunged from nearly $27 billion US dollars in 2000 to $15 billion in 2010.[[10]](#footnote-11)

Cite RIAA/IFPI stats – be quantitative

However, we must separate those losses from general declines in the business of the industry.

Use http://papers.ssrn.com/sol3/papers.cfm?abstract\_id=1932518 here (not just what the paper says but what sources it uses)

Sky is Rising paper <http://www.techdirt.com/skyisrising/> takes the contrarian view which we should include as well

[http://www.ipi.org/ipi\_issues/detail/the-true-cost-of-sound-recording-copyright infringement-to-the-us-economy](http://www.ipi.org/ipi_issues/detail/the-true-cost-of-sound-recording-piracy-to-the-us-economy)

<http://www.oecd.org/sti/38707619.pdf>

<http://www.cato-at-liberty.org/how-copyright-industries-con-congress/>

[http://www.hollywoodreporter.com/news/copyright infringement-costs-megaupload-kim-dotcom-318374](http://www.hollywoodreporter.com/news/piracy-costs-megaupload-kim-dotcom-318374)

[http://www.washingtonpost.com/blogs/ezra-klein/post/how-much-does-online-copyright infringement-really-cost-the-economy/2012/01/05/gIQAXknNdP\_blog.html](http://www.washingtonpost.com/blogs/ezra-klein/post/how-much-does-online-piracy-really-cost-the-economy/2012/01/05/gIQAXknNdP_blog.html)

<http://www.mpaa.org/resources/5a0a212e-c86b-4e9a-abf1-2734a15862cd.pdf>

<http://www.gao.gov/products/GAO-10-423>

Review the studies and try to mediate an explanation; I’ve started outlining the various arguments below

How does copyright infringement affect non-content industries (possibly include)

There can be other explanations besides just copyright infringement which are causing a change. Some may be linked to technology. For example, the shift to people listening to music on iPods could have changed the way people listen to music (any studies). On iTunes people can just buy a single popular track instead of buying the entire album (any studies?). This naturally leads to less revenue.

Another effect in the motion picture industry is that rental sites such as Netflix and Redbox are decreasing the demand for DVDs. (I know this from my summer at Disney, but any public info?)

On TV people are spending more of their entertainment time surfing the Internet than watching television (studies). This naturally leads to a drop in the amount of hours people watch television, leading to a drop in advertising rates. DVRs, such as Tivo, have also changed television watching by allowing users to time-shift their favorite shows and fast forward through commercials. Advertisers don’t like this and exempt these viewers from viewership data (cite).

In some ways

##### What are the Costs of Copyright Infringement?

We must be careful about what the costs of copyright infringement are. Many studies just cite the cost of copyright infringement as the list price of the item being stolen.[[11]](#footnote-12) However, there are multiple problems with that. First, as any economist will tell you, the number of people who demand a particular good is inversely proportional to the price. For example, standard economics tells us that less people will buy a CD priced at $20 than at $10. It follows then that many more will “buy” something if it is free. In fact, the difference between 1 cents and free is pretty substantial according to Dan Ariely in the New York Times bestseller Predictably Irrational.

###### Marginal Price

Copyrighted content has no to very little marginal cost. This opens up an entirely new type of pricing model compared to traditional industrial goods. It also makes losses due to copyright infringement more interesting.

Electronic copies of information are considered by economists to be “non rivalrous.”[[12]](#footnote-13) This means that one person’s enjoyment of a good is not diminished by another individual’s enjoyment of that good. Infinite perfect copies can be made of electronic goods. Giving a copy of an MP3 file to a friend does not diminish your ability to still listen to an MP3 file. In addition, whereas stealing a copy of a music CD at Walmart prevents Walmart from selling that copy to someone else, downloading a song from BitTorrent does not prevent others from accessing that song.

One could also make an argument about the different in cost accounting between the two. In the Walmart case, Walmart has prepaid for some number of CDs from the distributor, say $6. It then sells the CD for $10. Thus stealing the CD has lost Walmart the $6 they paid wholesale and the $4 profit they would have made on the sale. In the online case, say iTunes sells an album for $10, with $6 going to the record company for each album sale. If one gets a CD from an illegal source, then one has deprived Apple $4 in lost revenue and the record label $6.

###### Revenue

But also a higher price may lead to more revenue, while also leading to higher copyright infringement costs. Say for instance a TV show has 1 million users who watch for free. The TV network makes $1 off each user in advertising. Revenue is $1 million, while the copyright infringement loss is 0. Then say the TV network switches to a paid model in which an episode costs $4. Say 300,000 take the deal, and 100,000 decide to switch to copyright infringement. 550,000 stop watching all together. The network would make $1.2 million in revenue, which is more than before. They would also point to $400,000 in copyright infringement “losses.” Under the new strategy, they are making more money than before, but also are experiencing copyright infringement.

The question then is if copyright infringement was made harder, how many of these 100,000 pirates would switch to the paying $4. As was discussed earlier, it is very likely not all 100,000 would now pay. But how many would?

Ideally, the networks would like to segment each person out by their willingness to pay. Say half of these 100,000 would be willing to pay $1. The network would not want to simply lower the price to $1 because then they would have 350,000 each paying $1, for revenue of $350,000 which is even worse than the ad-supported model. But if they were able to get the original 300,000 to pay at the old price, plus the 50,000 at $1 then they would have $1.25 million in revenue, and copyright infringement losses of $50,000. Revenue is up, and losses due to copyright infringement are down.

##### Tracking Copyright Infringement

It is difficult to know exactly how much copyright infringement is going on because it is hard to track the transfer of pirated materials online.

Expand

?some studies on network traffic of BitTorrent – but then how much is pirated?

### Artists

There is some disagreement on how much money actually goes to artists.

That book I have

Do we want to cut this?

### Employment

How to measure

Another area for contention is how much profits at record labels actually lead to employment. The industry argues that additional profit allows them to invest more in the future, leading to more employment for artists. Cite/explain

Others claim that industry profits are unlikely to be redirected to \_\_\_\_\_\_.

For example, some look at the last 10 years of the industry. Profits are down XX%, but employment only XX%. Where did the lost value go to? How sustainable is that in the long run?

This has been controversial because some studies have cited a larger impact in jobs than the number of people who are actually employed by the music industry.

In addition, employment studies often try to include the “multiplier effect” of jobs. For example, person who works in the record industry spends money

Cite RIAA stats

Cite/explain

#### Money Redirected

Some argue that the money saved by consumers by not buying CDs is spent on other things. For example, rather than spending $10 on a CD, a consumer uses that same discretionary income to buy a sandwich instead. If the user would have spent the money on a CD, they would have not bought a sandwich. Thus the economic, including employment effect is merely transferred across industries, and does not actually hurt the economy.

Cite/explain

## Technical

1. Has minimal negative repercussions on internet
2. e.g. DNS

### Internet Infrastructure

Any proposal should not weaken the underlying infrastructure of the internet. For example, the above described proposal would have big effects on the internet.

?move what DNS is and how easy it is to cirmcvment here? Don’t think so, but draw a better distinction between the sections

The current DNS model, described above, is insecure. Results are returned without the use of cryptography. This means that an attacker could modify results before they are returned to a user. Unless the site uses SSL, one would not know that one was connected to the wrong site. The browser would still show the same URL, for example, google.com. The attacker could then ask for the user’s log on information which the user might still provide because the site’s visible URL is correct. The attacker could then use that information to steal the user’s account on the real site. An attacker could also post a fake order page to collect credit card numbers.

Recently there has been a push to extend DNS to also use cryptography. This effort is called DNSSEC.[[13]](#footnote-14) DNSSEC adds a chain of cryptographically signatures to responses.[[14]](#footnote-15) DNSSEC is seen as critical to securing the US’s Internet infrastructure, because it hardens the DNS system against fraud and other cyber-attacks. The White House released a memo in 2008 instructing all agencies to turn on DNSSEC.[[15]](#footnote-16) In addition, the Department of Homeland Security Cybersecurity R&D department has a program to encourage the deployment of DNSSEC.[[16]](#footnote-17)

The DNSSEC system has been purposely designed so that only the owner of a domain can sign a domain query to prove that it is valid.[[17]](#footnote-18) Thus only the author of the site can specify where the DNS service should resolve to. In addition, the system is set up so that if someone refuses to return a response, or submits an invalid response, the DNS service will continue to contact other DNS servers until it finds a valid response.[[18]](#footnote-19) The DNS system was designed to be resilient to interference! In addition, it was described earlier how this entire system is easily subvertable by a user purposely seeking “darknet” responses. Because of this, organizations such as the Association of Computing Machinery have spoken out about the dangers that the DNS blocking specified in SOPA would harm the Internet.[[19]](#footnote-20)

### How in infringement detected today?

Copyright owners detect copyright infringement in a variety of ways.

Where is best to put this?

#### P2P

By its nature, a peer-to-peer network makes available the list of IP addresses which are participating in sharing the file. In court cases, the record industry has used a firm called MediaSentry to monitor P2P networks.[[20]](#footnote-21) MediaSentry logs onto these networks and searches for a file known by their client to be infringing content.[[21]](#footnote-22) MediaSentry then receives the list of users who have parts of the file available from the P2P service’s tracking server.[[22]](#footnote-23) By seeing that the user has the file and is making it available to other users, MediaSentry can claim that the user is making the file available to others.

In other cases, MediaSentry attempts to actually download the file to verify that the content of the file is in fact copyrighted.[[23]](#footnote-24)

As a result, some people use IP blocking software such as PeerGuardian, and its successor PeerBlock.[[24]](#footnote-25) This software contains the list of IP addresses known to be used by Government, large businesses, and anti-P2P contractors such as MediaSentry. The software attempts to prevent those IP addresses from connecting to your computer to download part of the file from you.

Others use what are called “private trackers.” These only allow pre-screened persons to participate in the download, including having access to the list of persons who have portions of the file available for download. Without being one of the people with access, MediaSentry and others firms would have no way of knowing who was participating in the download.

#### DPI

However, one organization that would know would be your ISP. Internet users purchase internet access from Internet Service Providers (ISPs). ISPs have access to all of your traffic as it flows across their network. Internet traffic is sent as a packet, which is like an envelope. On the outside of the envelope, the packet has the IP header which specifies where the packet is sent among other things. The inside of the packet contains the actual message. Normally, ISPs only look at the header of the packet in order to forward it onward. However, with modern equipment ISPs can also look at the contents of these packets, as long as they were not encrypted. This was always possible, but it is only recently that it is possible to do at the scale required.

Protocol encryption makes it more difficult for ISPs to identify BitTorrent traffic. However, it can only work if the tracker and the other clients also support encryption. In addition, it has been shown that many BitTorrent clients still put out a characteristic file flow that ISPs can identify if they so wish.[[25]](#footnote-26) However, this only shows that the user is using BitTorrent, but not which file they are downloading. As the other section of the paper showed, BitTorrent can be used for non-infringing uses.

In 2007, Comcast was found to be using the “Fairshare” product from Sandvine which actively interfered with BitTorrent traffic.[[26]](#footnote-27) Sandvine captures a copy of the list of peers returned from a tracker. When a user tries to contact these nodes, their technology sends fake TCP reset packets – the equivalent of a fake hang up signal on a telephone. The action was controversial, and received a fine from the FCC for unfairly blocking a particular protocol.[[27]](#footnote-28)

All this is interesting, but where is best to put it?

## Minimally necessary

1. Is it the minimum necessary?
2. Non-infringing use of technology – effects on innovation (e.g. Megaupload, torrents)
3. Fair use arguments (creative/cultural)

A measure should be the minimum necessary to block copyright infringement, without impacting legitimate uses of a technology or service. It is often impossible to achieve a perfect separation between blocking infringing and non-infringing uses. Technology is technology. It does not care what the content is. A BitTorrent tracker can point to any file, either a political document or a copyrighted movie. In addition, there often with the same file certain uses are allowed, while others are not. For example, with a CD you can put a copy of a song on your iPod, but cannot give it to a friend. This further frustrates, often to the point of impossibility, the development of additional technology to prevent copyright infringements. In addition, some services have both infringing and non-infringing uses. For example, a file hosting site can hold a Hollywood movie or a home movie. Even determining what is copyrighted is often a challenge, because there is no one single repository.

### Non-infringing use

Many services which make copyright infringement easy can also be used for non-infringing use.

#### Sony/BetaMax

The canonical example is the Sony Corp. of America v. Universal City Studios, Inc. case.[[28]](#footnote-29) In this 1984 case, the Supreme Court of the United States found that Betamax machines have “significant non-infringing uses.” First off, the Court found that the producers of the devices were not liable for the actions taken by the purchasers of the device:

sale of copying equipment, like the sale of other articles of commerce, does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes

Even though some people may use it to infringement:

the business of supplying the equipment that makes such copying feasible should not be stifled simply because the equipment is used by some individuals to make unauthorized reproductions of respondents' works

Furthermore, the time shifting feature of the devices is allowed:

one potential use of the Betamax plainly satisfies this standard, however it is understood: private, noncommercial time-shifting in the home. It does so both (A) because respondents have no right to prevent other copyright holders from authorizing it for their programs, and (B) because the District Court's factual findings reveal that even the unauthorized home time-shifting of respondents' programs is legitimate fair use

Thus the Betamax, and its close cousin the VCR were allowed to be sold as long as people could use the service for non-infringing use. In the end, the VCR launched a huge market in not just pre-recorded Hollywood movies, but also in VHS cameras. In 1984 JVC released the first consumer camcorder which allowed consumers to record directly to VHS tape, which they could play back on their VCRs.[[29]](#footnote-30)

##### BitTorrent

Another example is BitTorrent. Although widely used to download copyright infringing materials, the protocol is also being used to quickly distribute large files without requiring much infrastructure. For example, game developers use BitTorrent to distribute updates to their games.[[30]](#footnote-31) These updates can be quite large (over 500MB). Traditionally companies would buy or rent many racks of servers to provide this content. In addition, these servers would require a lot of bandwidth. As bandwidth grows scarcer, this is becoming a growing concern. Under a BitTorrent model, the company only has to *seed* a few updates to members of the community around the world from their own servers. Other players then download a copy of the update from other users. Not only does this save the game company from requiring extra bandwidth, it also makes the download for the user, especially in countries with limited bandwidth. This is because the file is being downloaded from someone nearby. In addition, this decongests the Internet, requiring less bandwidth. It is win-win scenario.

#### Megaupload

One example of a case that is currently in progress is Megaupload. Megaupload was a direct-file hosting and download site. Users upload file to Megaupload and then receive a URL. Users could use the site to transmit files larger than email. They could send the URL they received to a friend or business colleague in an email message. Because the actual file was not attached to the email, the email is small enough to be sent on almost all systems. For example, a video production house might use Megaupload to distribute a preview copy of a video to a client. Persons could also use Megaupload as a backup service. They could upload a copy of their important files to Megaupload. If their computer were to crash, they could visit Megaupload again to download the file.

Kyle Goodwin was a MegaUpload user who lost his files when his hard drive crashed.[[31]](#footnote-32) Mr. Goodwin is a videographer. He used Megaupload as a backup service for his videos. Shortly before the government’s January raid, Mr. Goodwin’s hard drive crashed. His only copies of his videos are the ones stored on Megaupload. However, the government is resisting restoring his files in court, claiming that some of the videos Mr. Goodwin produced had copyrighted songs as their soundtrack.[[32]](#footnote-33) Furthermore, the government is arguing that people do not acquire an ownership interest by uploading songs to a service.[[33]](#footnote-34)

### DRM

DRM is a good example of technology that limits what honest consumers can do. Music sold on iTunes used to be protected with “FairPlay” DRM. That DRM restricted purchasers of the music to only being able to maintain listenable copies of that music on up to five computers.[[34]](#footnote-35) However, the music could only be played on devices that supported FairPlay, namely iPods, iPhones, and computers with iTunes installed.[[35]](#footnote-36) Other brands of devices were not supported as they did not have the capability to play FairPlay files and Apple refused to license it to others.[[36]](#footnote-37)

Thus DRM served only to frustrate the purchasers of legitimately purchased music. As discussed above, illegally gotten tracks were not only free, but came without these strings attached. A proposal should not add this sort of incentive.

### Fair Use

Proposals should not add chilling effects on legitimate uses of copyright technology. For example, United States law permits fair use.

**17 U.S.C. § 107**

Notwithstanding the provisions of sections 17 U.S.C. § 106 and 17 U.S.C. § 106A, the fair use of a copyrighted work, including such use by reproduction in copies or phonorecords or by any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright. In determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include:

1. the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;
2. the nature of the copyrighted work;
3. the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
4. the effect of the use upon the potential market for or value of the copyrighted work.

The fact that a work is unpublished shall not itself bar a finding of fair use if such finding is made upon consideration of all the above factors.

Fair use suffers from a few practical problems. First off, what is fair use and what is not are not laid out explicitly in the statue. As a result there have been a long string of cases which attempt to provide guidance on what is fair use and what is not.[[37]](#footnote-38) For example, a work that parodies a second work is protected against infringement claims by that second work, but a work that parodies society in general by using a second work is not protected.[[38]](#footnote-39)

#### Beforehand/Afterhand

As such it is almost impossible to determine if a particular use of a material qualifies as fair use.

Many of today’s technologies do not account for fair use. It is especially difficult for a computer to determine if these tests are met. This many services, such as Google’s YouTube take down the content first.

For example, YouTube’s Content ID system does not account for fair use before a work is removed.[[39]](#footnote-40) It is only after a work is removed, that the uploader may go to YouTube and contest the removal of the work. One of these options is that the work falls under fair use protection. The uploader can then describe why they feel the work should receive fair use protection. A YouTube employee then reviews the rationale and decides whether or not to accept the rational. If the rational is accepted, the video remains as is. If the rational is rejected, the blocking remains.

Note that a YouTube content ID match does not necessarily mean that one’s content is removed. Instead, the content may be blocked only in certain countries, may have ads shown next to it, or part or all of the audio may be muted.

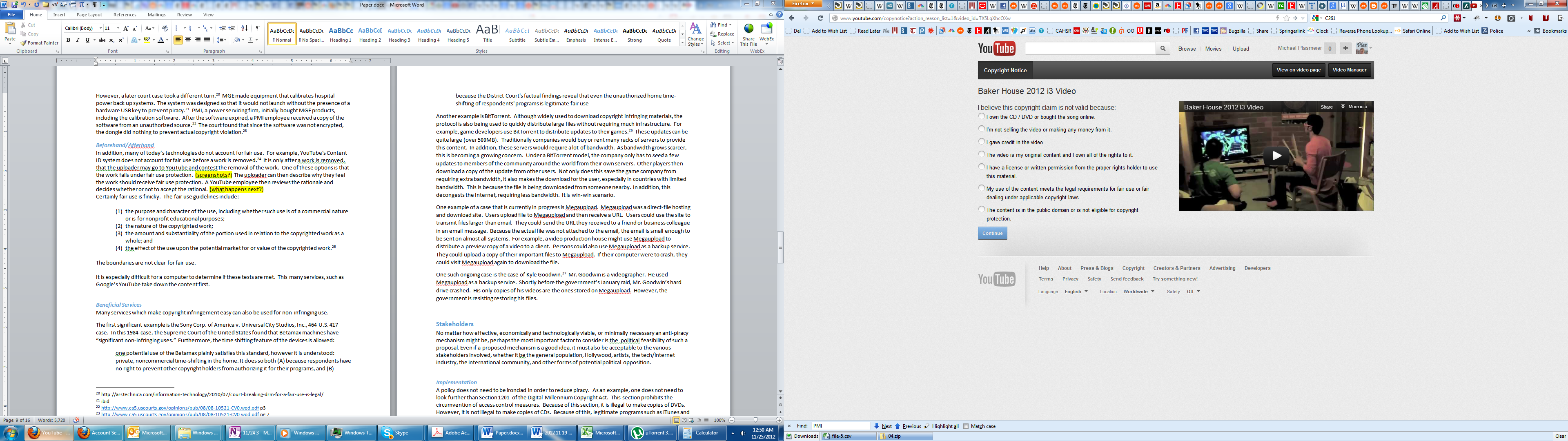


Figure 1 YouTube Content ID Copyright Claim Invalid Page

#### Fair Use and the DMCA

In addition, fair use does not overrule the DMCA. In Universal City Studios v. Reimerdes, the court stated that "[i]f Congress had meant the fair use defense to apply to such actions, it would have said so."[[40]](#footnote-41) Thus one is not permitted to remove the encryption on media such as DVDs to make a copy under the normal provision of fair use.

##### Section 1201 Process

Instead, Congress does allow for encryption to be broken, but under a more limited set of criteria than fair use. This is spelled out in Section 1201 of the DMCA.

Section 1201 requires that every three years, the Library of Congress must hold hearings in which citizens can ask for exemptions of the DMCA to break encryption in certain specific cases.[[41]](#footnote-42) For example, in the most recent rulemaking, the Federal Registrar stated that:

“The primary responsibility of the Register and the Librarian in this rulemaking proceeding is to assess whether the implementation of access control measures is diminishing the ability of individuals to use copyrighted works in ways that are not infringing and to designate any classes of works with respect to which users have been adversely affected in their ability to make such noninfringing uses.”[[42]](#footnote-43)

Specifically the Register and the Librarian are to look at:

1. The availability for use of copyrighted works
2. the availability for use of works for nonprofit archival, preservation, and educational purposes
3. the impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research
4. the effect of circumvention of technological measures on the market for or value of copyrighted works
5. such other factors as the Librarian considers appropriate.[[43]](#footnote-44)

However, the process is heavy in bureaucracy, taking about one year from initial notice to final rules published in the Federal Registrar.[[44]](#footnote-45) Congress requires that the Register and the Librarian solicit input from a wide range of stakeholders in consideration of a “broad range of current or likely future adverse impacts.”

In addition, exemptions expire every 3 years and thus must be reargued each time.

#### Real DVD

Other services which broke encryption on DVDs for claimed fair use purposes were later found to be illegal. RealNetworks, a maker of media playing software, had tried to launch RealDVD back in 2008.[[45]](#footnote-46) RealNetworks is a legitimate company, who had a license to play back DVDs. The software was designed to allow users to rip DVDs and watch them on their computers.[[46]](#footnote-47) Real then added an additional layer of copy protection to ensure that users could only play the movies on up to 5 devices.[[47]](#footnote-48)

The judge disagreed with RealNetwork’s fair use assertion, writing “Fair use is not a defense to trafficking in products used to circumvent effective technological measures that prevent unauthorized access to, or unauthorized copying of, a copyrighted work.” [[48]](#footnote-49)

## Stakeholders

No matter how effective, economically and technologically viable, or minimally necessary an anti-copyright infringement mechanism might be, perhaps the most important factor of all to consider is its political feasibility. Even if a proposal is deemed to be a good idea, it must also be acceptable to the various stakeholders involved, whether it be the general public, Hollywood, artists, the tech/internet industry, the international community, and other potentially affected players. To ignore the multiplicity of opinions among the key players is to assume a perfect conveyance of policymakers’ decision-making logic to their constituents; this is simply not the case. While such simplifications “make normative analysis possible and useful at the individual level [they] can become serious deficiencies in the study of public policies” (Majone, 1975).

Moreover, the inclusion of political feasibility assessment in technical policy analyses has been said to “enhance the probability that the technical analysis contained therein will be considered” (Webber, 1986). The neglect of technical factors in ongoing anti-copyright infringement legislative debates is, after all, one of the central deficiencies we hope to remedy with our evaluative framework. As such, political factors play a significant role in our evaluative framework for anti-copyright infringement measures.

This branch of our analysis will take place on two l­­evels, examining the political details of the proposal itself as well as possible political reactions to it. First, we will look at the actors(s) assigned the responsibility of implementing the mechanism in question: do they have the proper authority to carry out the proposed operations, and who is to bear the resulting financial burdens? Second, the assessment will analyze the various key players to anticipate the level of political resistance a policy might encounter: what motivations, belief systems, and resources do each of the stakeholders have, and how might they react to the proposed mechanism? This two-pronged approach of political feasibility analysis will allow for a comprehensive assessment of whether a given policy will be likely to gain the support necessary for passage and, eventually, implementation.

### Responsibility of Implementation

When assessing the effectiveness of an anti-copyright infringement mechanism, one must not only look at the actual effects that the proposal might have. It is also imperative to ensure that the mechanism can be implemented with ease, can be sustained for a sufficient amount of time to have a lasting effect on online copyright infringement, and is robust enough for future modification or extensibility to new conditions and scenarios. This is a matter of identifying potential opposition to a proposed measure both based on the current political climate as well as predicting future challenges that it may encounter down the line. Issues of efficacy are perhaps better addressed by the economic and technical portions of our evaluative framework. The analytics we will focus on in this section are based more on assessing the political legitimacy of a proposal—a notion that is largely encapsulated by how the responsibility of implementation is allocated among government and relevant stakeholders.

### *Proper Authority/Jurisdiction*

In our political analysis, we’ll first look at whether or not the actor(s) assigned the responsibility of implementation actually has the necessary authority to do so. This criterion embodies a number of questions about established powers, legal precedents, and political jurisdiction. In more concrete terms, our framework favors proposals whereby the implementation clearly falls within the scope of what the governmental agency or actor was intended to address. The goal here is to eliminate overbroad or overreaching policy measures, as they are more likely to be politically volatile. In particular, vague or ambiguous language is to be avoided; the details of a policy’s implementation should be narrowly defined enough that it obviously falls within the purview of that office’s political authority. Those proposals that do not meet these criteria are far more likely to meet resistance from critics and will suffer from a loss in overall political feasibility.

As an example of an anti-copyright infringement mechanism that would fare poorly on this metric of authority and jurisdiction, take something like the Anti-Counterfeiting Trade Agreement (ACTA), an international trade agreement that establishes global standards on intellectual property enforcement. Negotiated in secret, ACTA circumvented the need for congressional approval and public scrutiny, thanks to its status as a sole executive agreement, “concluded on the basis of the President’s independent constitutional authority alone” (Katz & Hinze, 2009). In short, the White House used this transparency loophole to enter the ACTA agreement without consultation. Naturally, the constitutional authority of such an action has been contested; thus, we see how questions of due process may play a role in determining the political acceptability of a proposed anti-copyright infringement mechanism.

### *Financial Burden*

Yet another important consideration to take into account is the parties that are assuming the financial burden associated with the proposed mechanism.

## Possible Political Resistance

Ultimately, the process of assessing political feasibility is one of comprehensive information gathering and synthesis. Using the model of analysis first laid out by Meltsner, we must consider the confluence of “(1) actors, (2) motivations, (3) beliefs, (4) resources, (5) sites, and (6) exchanges” to determine “which actors will be politically effective, which will exercise power… [and] the possible areas of policy consensus and conflict” (1972). This will allow us to develop a map of the political climate surrounding a specific policy proposal and identify potential pathways (if any exist) of moving forward with it. While the issue of online copyright infringement spans multiple policy spaces and eludes a single generalized case, we can identify the most prominent or likely elements in each of these categories and still leave room for additional flexibility.

Actors, motivations, beliefs, resources, sites, exchanges specific to the anti-copyright infringement debate

### Synthesis

Once all the aforementioned factors have been determined and detailed, we may begin synthesizing all the information to assess the overall political feasibility of the proposed mechanism. There are a multitude of models for conflict resolution in decision-making. Majone suggests that the best public decisions are those that consider not only the technical, economic, and legal limitations of a proposal, but also a "distributional constraint" like Pareto admissibility (1975):

A decision affecting a number of people is said to be Pareto admissible if there is no other feasible decision that is preferred by one or more persons, and if nobody regards it as inferior... A change from state S to state S1 is Pareto admissible if, in the transition, either every person in the relevant group is made better off, or at least one person is made better off, and nobody is made worse off. Notice that the change from one state to another can be Pareto admissible even if the states themselves do not satisfy the Pareto criterion.

Example of applying Pareto admissibility criterion based on previous subsection

# Meta-analysis of Framework

Strengths, weaknesses, possibilities for future improvement

# Current Policy Debates

The possibility of a graduated response to copyright infringement started in mid-2007 in France.[[49]](#footnote-50) Nicolas Sarkozy, the newly elected President of France appointed an independent review commission to review copyright infringement.[[50]](#footnote-51) That commission was run by the pro-enforcement Denis Olivennes.[[51]](#footnote-52) The commission found that P2P was killing France’s culture and sought to do something about it. The commission modeled their approach on the “three strikes and you’re out” feature of baseball.[[52]](#footnote-53) After 2 warnings, a user could be disconnected from the internet.

I don’t know why I put this here. I wanted to do an intro to graudated response, but it’s really an intro to HADOPI

## HADOPI (Stephen)

http://arstechnica.com/tech-policy/2008/06/frances-three-strikes-copyright-law-gets-cabinet-support/

##### Effects of HADOPI Law in France

One study conducted by researchers at Wellesley College and Carnegie Mellon University looked at the implementation of the Hadopi law in France and compared the sales of music on iTunes with other European countries who did not have a similar law.[[53]](#footnote-54) The study found a 25.5% increase in track sales in the control group, but a 48% increase in France, indicating that sales were 22.5% higher in France then the rest of Europe, likely due to the Hadopi law.[[54]](#footnote-55) There was a similar result for album sales.[[55]](#footnote-56) Additionally this general trend was true for all labels, so it’s unlikely that these effects were due to a particular artist being popular in France.[[56]](#footnote-57) In addition, these results did not occur when other countries were isolated.

(also explore what sources it uses)

The study also looked particular genres of music. First the study looked at a survey taken by EMI which asked people how much they are likely to pirate each type of genre of music.[[57]](#footnote-58) They then found the largest sales increase in genres which were reported to be heavily pirated.[[58]](#footnote-59) For example, Rock and Pop were both the genres most pirated, and the genres which experienced the largest increase in sales after the HADOPI law than before the law.

This shows that it is unlikely that there is any other explanation for this phenomenon than the HADPOI law. For example, increased sales in France suggest that Apple could have just heavily started promoting iTunes in France. But this genre comparison suggests that it is an unlikely explanation. It is also interesting to note that the lines started diverging right as parliament started debating HADOPI, not when it came into force. In addition, when this study was written no one had yet received a third/disconnect notice.[[59]](#footnote-60)

Bhattacharjee et al showed an awareness of copyright infringement lawsuits did cut the number of pirates, but found that the effect was short-lived.[[60]](#footnote-61)

## 6 Strikes vs Lawsuit – Plaz

In early July 2011, the RIAA and the MPAA signed a voluntary agreement with many of the country’s largest Internet Service Providers (ISPs) to introduce a “6 Strikes” graduated response system to the United States.[[61]](#footnote-62) The system is officially called the Copyright Alert System or CAS, but in the popular press, the name “6 Strikes” is often used.

### Description

Under the system, copyright owners could make complaints against IP addresses to users.[[62]](#footnote-63) ISPs will then forward those complaints on to users – without actually revealing information about the user to the copyright holder. [[63]](#footnote-64)

The “6 Strikes” system establishes the Center for Copyright Information (CCI). The center is tasked with administering the CAS as well as educating the public on copyright issues.[[64]](#footnote-65) The Center is governed by a 6 member advisory board, with 3 members appointed by the content industries and 3 members from Internet Service Providers.[[65]](#footnote-66) There is also a four member advisory board, with members from the Center for Democracy and Technology, Public Knowledge, iKeepSafe, and the Future of Privacy Forum.[[66]](#footnote-67) Reports indicate that these members are serious about a balanced approach and are independent from the other players.[[67]](#footnote-68) However, these members are only advisory. The executive board has no requirement to listen to them. [[68]](#footnote-69) The MOU also requires the executive committee to retain independent technical experts.[[69]](#footnote-70) The MOU prohibits sending alerts from methods deemed to be “fundamentally unreliable.”[[70]](#footnote-71) However, the names of these experts is not public. In addition, the reports generated by the experts are not required to be public.

Under the CAS, Copyright owners provide ISPs with documented evidence of infringement.[[71]](#footnote-72) However, there is no common standard format or implantation plan. Instead, each ISP is able to define their own implementation form and data format.[[72]](#footnote-73) Each ISP is also able to define what each of the six strikes definitively means. However, the MOU lays out an outline of what each strike could be.

The first two alerts are purely educational.[[73]](#footnote-74) They do not require any response or action form the user. The alerts will contain information that copyright infringement is illegal, that there are lawful ways to download content, and that further sanctions may follow. The third and fourth alerts also educate the user, albeit in stronger language.[[74]](#footnote-75) They also require the user to take some affirmative action to close the alert.

Finally with the last two alerts, “mitigation measures” or “sanctions” can be taken. The MOU does not mention specific sanctions, but instead offers a menu from which ISPs can choose:

Such measures include, but are not limited to, a temporary reduction in transmission speed, a temporary step-down in the subscriber’s service tier, a temporary redirection to a landing page for completion of a program of copyright instruction, a temporary redirection to a landing page until the subscriber contacts a customer service representative, or a temporary suspension of access.[[75]](#footnote-76)

Unlike some media reports, ISPs are not required to suspend a user’s internet access.[[76]](#footnote-77) Instead the ISP may decide which sanctions to implement. Notices reset after 12 months without receiving an alert.[[77]](#footnote-78) Seven days are allowed between each alert that counts towards the six.[[78]](#footnote-79)

#### Appeal Process

After getting a fifth and sixth notice, a user has 14 days to file an appeal via an “Independent Review Program” before the mitigation measure is imposed.[[79]](#footnote-80) The Independent Review Program is a non-judicial program set up by CCI with the American Arbitration Association (AAA).[[80]](#footnote-81) The overhead of the program is paid by CCI, which is funded equally by content groups and by ISPs.

A user can also appeal their first through fourth notices upon receiving their fifth notice.[[81]](#footnote-82) However, if a user does not appeal those earlier notices at that time, then they cannot again appeal those in the future.[[82]](#footnote-83)

In order to file an appeal, a user fills out an online “Application to Commence Independent Review” or “ACIR” form.[[83]](#footnote-84) In addition, a user must pay a $35 fee on appeal, however, such fee is refundable if a user prevails in their appeal.[[84]](#footnote-85) The user may select from 6 possible defenses:

1. account misidentification
2. unauthorized use of account
3. authorized use of content
4. fair use
5. misidentification of content
6. work published before 1923[[85]](#footnote-86)

The user must include a basis for each defense and possibly provide the corresponding backup material.[[86]](#footnote-87) For example, if a user asserts authorized use, the user must provide specific, written authorization. If a user claims fair use, then they must provide (1) a copy of each file, and (2) an explanation of each use, and the basis for claiming fair use.

The ISP and the Copyright owner will also be able to submit information.

The review process is designed to be automated; in addition one reviewer per case is selected by the AAA.[[87]](#footnote-88) Reviewers must be lawyers, but they are not required to have specific copyright experience.[[88]](#footnote-89) However, they are required to have training from a CCI-Approved Copyright expert.[[89]](#footnote-90)

### Analysis

#### Is effective in reducing copyright infringement?

We believe that this method will be effective in reducing copyright infringement (look at Hadoopi).

Compared to the previous system where the content industries directly sued users the new system is much more scalable. Under the old system, companies had to file individual John Doe lawsuits in order to ask a court to unmask a user’s identity.[[90]](#footnote-91) The case could then go to a lengthy and expensive trial.[[91]](#footnote-92) Although in many cases, the user settled by paying an average of $3,000.[[92]](#footnote-93) This was not cost effective for the industry.[[93]](#footnote-94) A TechDirt study of RIAA financial records found that the RIAA spent over $17.6 million dollars on lawyers in 2008.[[94]](#footnote-95) As a result, the RIAA brought in $391,000 in settlements.[[95]](#footnote-96) The industry did it because they believed it would be a disincentive for users to illegally download files.[[96]](#footnote-97) The new system seems much more efficient in comparison.

Under the old system, two plaintiffs attempted to fight instead of settling. Joel Tenenbaum, a student at Boston University, was found to have willfully infringed by downloading 30 songs over KaZaA in 2003.[[97]](#footnote-98) The jury awarded the music companies $675,000, or $22,500 per song, a substantial discount over the $150,000 statutory limit.[[98]](#footnote-99) Jammie Thomas-Rasset, was found guilty of copyright infringement of 24 songs for statutory damages of $1.92 million dollars, or $80,000 per song.[[99]](#footnote-100) This was later reduced to $54,000 or $2,250 per song, and then increased to $222,000.[[100]](#footnote-101)

In trials, defendants have claimed that others performed the actual infringement, for example, though an unsecured WiFi network. When a plaintiff files a John Doe lawsuit with an ISP, they receive the name of the subscriber who is paying for the internet connection. Courts in Finland have found that this is insufficient to prove guilt, as it does not show that the person actually performed the infringement.[[101]](#footnote-102) The EFF also argues that merely providing open WiFi does not make someone liable for copyright infringement.[[102]](#footnote-103) In addition, the EFF argues that the DMCA provides a safe haven for service providers who offer “the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user’s choosing, without modification to the content of the material as sent or received.”[[103]](#footnote-104) This was originally written for large ISPs, but the EFF argues it applies just as well to small providers of WiFi hotspots.

Unfortunately this provides an open loophole in preventing copyright infringement. Although legally there is no negligence defense for copyright infringement, this allows persons to avoid liability, harming protection against copyright infringement.[[104]](#footnote-105) We feel there is some distinction between a business that regularly provides free wifi and an individual that keeps his WiFi open as a defense.

(wandering off topic; where is best for this?)

In addition, court cases have tried to distinguishing actual transmission of the file versus making available. MediaSentry has a hard time showing that the file was actually transmitted using the methods that they employ. If they were to actually download the material, that raises questions about whether it is an illegal act to transmit a copy of the work to an agent of the work.[[105]](#footnote-106) Courts at first ruled in the Olan Mills, Inc. v. Linn Photo Co. that this was legal, however then made an exemption for investigators in RCA/Ariola Int’l, Inc. v. Thomas & Grayston Co., 845 F.2d 773, 781‐82 (8th Cir. 1988). So the courts rejected such an argument in the Thomas case.[[106]](#footnote-107)

At some point we should decide whether or not these defenses should be allowed. These should not be established behind closed doors by the Copyright and ISP industries. Instead, the process of what defenses should be allowed should occur in the public eye.

The Courts are generally where this case law has been established. However, this is a lengthy process. Though generally, only one person needs to go through this process to establish the case law in the first place. That is why this method of allowing motivated parties to sue and go through the long precedent setting process, while allowing others to quickly move through the process is a good one. After one party has established the rules, the others just need to follow them.

For example, should the use of open WiFi access points be allowed? Does making available constitute infringement, or must it actually be transmitted?

Another process that could work is the same one used by administrative agencies to issue new laws. Here agencies here from all parties and then try to craft the best solution from the information they have received. This is a good way to trade off the costs of a policy with its benefits.

Once this policy has been established, we should move to a scalable process that allows the law to rapidly be applied.

(the last 4 paragraphs need rearrangement)

(this is prob not the right place for all this content)

#### Does the policy make economic sense?

The proposal appears to cost very little. In particular, the system attempts to automate as much of the process as possible - it is built for scale. The cost would be mostly in the initial setup of the system.

By having a low cost, the system only needs to stop a little amount of copyright infringement in order to be cost effective.

It is also much more fair to individual defendants. Even the minimum $750 per song is much too high. A controversial report by the Republican Study Group made the same assertion.[[107]](#footnote-108) The initial settlement amounts of $3,000 for about 30 songs ($100 per song) looks very good compared to the amounts which could be lost in courts (minimum of $750 per song, not including legal fees).

On the other side, some lawyers does not actually try to seek lawsuits; instead seeking to settle with as many people as possible.[[108]](#footnote-109) Some judges have sought to block this model, by requiring lawyers to file one-by-one, incurring a filing fee each time.[[109]](#footnote-110) Other judges have become angry that these cases took up space on their docket and threw out the entire lawsuit.[[110]](#footnote-111)

Both of these incentivize non-guilty parties to settle as much as guilty parties. That is not how the court system is supposed to work. This process is too heavy and burdensome for the courts.

#### Does it have minimal negative repercussions on the Internet?

rearrange

This depends on how the policy is implemented. In the past, some ISPs have intercepted pages and have added banners onto pages in midflight.[[111]](#footnote-112) For example, in 2008 Rogers added a quota message to the top of the Google home page by inserting Javascript into the page using an active version of Deep Packet Inspection. This technology is sold by companies such as PerfTech.[[112]](#footnote-113) Many (who) find the practice of modifying other sites’ pages over the Internet to be abhorrent.[[113]](#footnote-114) (expand)

Put elsewhere

Meanwhile almost all wireless access points use some sort of redirection technique to bounce first time visitors to a log in page. For example, many services send back a false DNS response, directing the user to the log in page instead. Or a user’s request is redirected by a HTTP redirect after a page is received. A user may also be redirected by IP address to the log in page. All of these techniques are not clean in regards to how the internet was designed. This can present problems. For example, my iPad tries to refresh my email and the WiFi router answers as the mail server. My mail server does present a security warning, but if the user clicks through, the access point could be trivially designed to intercept my mail credentials.

However a similar technique may pose problems for the internet. For example, a user may be uploading data in the background when their internet connection is redirected to this message – causing the update to break. Or perhaps a user is connecting to a computer via remote access when the redirection happens. If the redirection is not properly implemented, it could break the remote access connection.

For example, Comcast’s Sandvine implementation ended up blocking some email transmissions sent with Lotus Notes, a less-popular email client made by IBM.[[114]](#footnote-115) Sandvine did not intend to block Lotus Notes from sending email, but the technique Lotus was using to transfer large attachment must have been similar to the BitTorrent network technique. It appears that Sandvine had never tested sending attachments over 2MB with Lotus Notes before rolling out their product.

It would impossible for Sandvine to test every possible network configuration. That is why we have standards! Standards abstract away complicated implementation details. Messing with these standards ends up breaking things and makes them harder to test.

The right DPI technology needs to be implemented to be able to show a message without breaking the internet.

ISPs are not looking for infringement themselves

These techniques could also impact security if they are not done properly. For example, adding poorly written JavaScript to another page could allow user-generated content on a page to break out of the containment that the author of the page provided. We have seen before that copy protection code can have unintended consequences. For example, Sony BMG released CDs in 2005 that contained MediaMax copy protection.[[115]](#footnote-116) This software was poorly written to hide all files on a user’s system starting with “$sys$.”[[116]](#footnote-117) A virus could use this $sys$ name to hide itself on all computers which had ever played CDs containing MediaMax.

#### Is it the minimal necessary? (we should rename this)

This technique still makes no attempt to filter out fair use requests ahead of time. Instead, a user must lend the AAA $35, fill out paperwork, and then wait for a response. The burden of proof of showing fair use is on the user.

It remains to be seen what technical measures are used to identify infringement. This will give us more information of whether it will alarm on the use of services that provide non-infringing use such as Megaupload. (didn’t they say just P2P?) (they also can’t use the same methods)

#### Is it acceptable to stakeholders?

Wait for Stephen’s section

#### Other/To-do

* 6 Strikes takes down content first. Can appeal as fair use – but only afterwards
* And only then on the 5th and 6th notices
* Likely be effective against main problem
* Good to educate people
* Good balance
* Should be able to complain easily
* Not so many long procedural hurdles
* Penalties small next to $1000 settlements or hundred k judgements
* Should be automated and streamlined
* But if you have a problem, should be able to reach someone who has authority over the phone
* The fact that the copyright expert needs to be CCI approved is troubling. Content industries have a long history of putting out biased, extreme, or just plain wrong information on copyright. (must cite/backup)

# Upcoming policy debates

When evaluating future policies to protect against copyright infringement, policy writes should consider the framework we have outlined above.

Republican Study Group

# Specific Policy Recommendation

TBD

Not just current policy, but what should be done

Should 6 Strikes be mandatory? (I’m thinking no)

Audience for proposal

Read about recent updates in 6 Strikes Implementation plan

Really need to write this section!

# Other

* Selling in one country vs another
* Damages larger than the entire past profits of the record industry
* Make more specific (Don Unger)
* Future/flux (Don Unger)
* Hollywood making $$ on VHS

# Share of work

Stephen wrote the proposal and stakeholders

Michael wrote everything else

# Cut Sections

However, a later court case took a different turn.[[117]](#footnote-118) MGE made equipment that calibrates hospital power back up systems. The system was designed so that it would not launch without the presence of a hardware USB key to prevent copyright infringement.[[118]](#footnote-119) PMI, a power servicing firm, initially bought MGE products, including the calibration software. After the software expired, a PMI employee received a copy of the software from an unauthorized source.[[119]](#footnote-120) The court found that since the software was not encrypted, the dongle did nothing to prevent actual copyright violation.[[120]](#footnote-121)

1. The law says nothing explicitly about “space shifting” your collection, for example, ripping a CD you own to put on your iPod. However, there has never been an explicit case brought against someone for ripping. In addition, at attorney for MGM said that his clients, the record companies, have no problem with people ripping a CD for their own personal use.

   Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd. (3/29/05), 04-480 http://www.supremecourt.gov/oral\_arguments/argument\_transcripts/04-480.pdf [↑](#footnote-ref-2)
2. dyn.com/sopa-breaking-dns-parasite-stop-online-copyright infringement/ [↑](#footnote-ref-3)
3. In normal operations [↑](#footnote-ref-4)
4. http://css.csail.mit.edu/6.858/2012/readings/trajectories.pdf [↑](#footnote-ref-5)
5. DNS normally works by contacting a hierarchy of name servers, starting from a central server. Normally people query this standard hierarchy. However, there is nothing which requires that they use this hierarchy. A darknet DNS is one where the user defines a different root DNS to look at, usually in addition to the normal DNS tree. If these servers were run entirely out of the US, they would be out of the reach of US law enforcement. [↑](#footnote-ref-6)
6. The interesting possible exception to this occurs interestingly enough in copyright law. Under the DMCA (17 U.S.C Sec. 1201(a)(1))it is illegal to remove the encryption and produce tools or parts of tools that circumvent encryption. In one case Memorandum Order, in MPAA v. Reimerdes, Corley and Kazan (NY; Feb. 2, 2000) (https://w2.eff.org/IP/Video/MPAA\_DVD\_cases/?f=20000202\_ny\_memorandum\_order.html the court claimed that the key in and of itself was a copyright circumvention device. A key, is at its base, just a very large number. In response, a number of people made an image with the colors of each section of the image being represented by the same digits as the encryption key. 46-dc-ea-d3-17-fe-45-d8-09-23-eb-97-e4-95-64-10-d4-cd-b2-c2 by Ben S, Yale Law Tech, 2011 Marchhttp://www.yalelawtech.org/trusted-computing-drm/46-dc-ea-d3-17-fe-45-d8-09-23-eb-97-e4-95-64-10-d4-cd-b2-c2/

   In addition, all computer files are, at their core, a string of 1s and 0s. These strings form very long binary “numbers” which it is illegal to posess. [↑](#footnote-ref-7)
7. http://www.cbo.gov/sites/default/files/cbofiles/ftpdocs/91xx/doc9197/hr4279.pdf [↑](#footnote-ref-8)
8. ibid [↑](#footnote-ref-9)
9. ibid [↑](#footnote-ref-10)
10. IFPI 2010 study including both digital and physical sales of recorded music [↑](#footnote-ref-11)
11. http://www.cato-at-liberty.org/hulu-pricing-strategies-and-the-costs-of-copyright infringement/ [↑](#footnote-ref-12)
12. Hess, C., E. Ostrom. 2006. Introduction. C. Hess, E. Ostrom, eds. Understanding Knowledge as a Commons: From Theory to Practice. The MIT Press, Cambridge, Massachusetts [↑](#footnote-ref-13)
13. http://usacm.acm.org/images/documents/DNSDNSSEC.pdf [↑](#footnote-ref-14)
14. Ibid pg 3 [↑](#footnote-ref-15)
15. http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2008/m08-23.pdf [↑](#footnote-ref-16)
16. http://www.cyber.st.dhs.gov/dnssec/ [↑](#footnote-ref-17)
17. Ibid pg 3 [↑](#footnote-ref-18)
18. Ibid pg 4 [↑](#footnote-ref-19)
19. Ibid pg 5 [↑](#footnote-ref-20)
20. http://blogs.law.harvard.edu/cyberone/files/2008/11/497-2.pdf [↑](#footnote-ref-21)
21. ibid [↑](#footnote-ref-22)
22. ibid [↑](#footnote-ref-23)
23. http://arstechnica.com/tech-policy/2009/01/mediasentry-may-be-gone-but-riaa-tactics-will-live-on/ [↑](#footnote-ref-24)
24. http://torrentfreak.com/peerblock-file-sharing-safety-tool-clocks-100000-downloads-091111/ [↑](#footnote-ref-25)
25. http://www.howtogeek.com/76801/how-to-anonymize-and-encrypt-your-bittorrent-traffic/ [↑](#footnote-ref-26)
26. https://www.eff.org/deeplinks/2007/10/comcast-also-jamming-gnutella-and-lotus-notes [↑](#footnote-ref-27)
27. http://www.pcmag.com/article2/0,2817,2326980,00.asp [↑](#footnote-ref-28)
28. Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417 [↑](#footnote-ref-29)
29. http://www.totalrewind.org/cameras/C\_GRC1.htm [↑](#footnote-ref-30)
30. http://torrentfreak.com/bittorrent-to-speed-up-game-distribution-080915/ [↑](#footnote-ref-31)
31. http://torrentfreak.com/u-s-accuses-megaupload-user-of-storing-pirated-music-121031 [↑](#footnote-ref-32)
32. http://arstechnica.com/tech-policy/2012/10/government-innocent-megaupload-user-uploaded-pirated-music/ [↑](#footnote-ref-33)
33. ibid [↑](#footnote-ref-34)
34. http://www.apple.com/support/itunes/store/authorization/ Retrieved 2008-09-13. [↑](#footnote-ref-35)
35. ibid [↑](#footnote-ref-36)
36. http://www.conseil-concurrence.fr/pdf/avis/04d54.pdf [↑](#footnote-ref-37)
37. http://fairuse.stanford.edu/Copyright\_and\_Fair\_Use\_Overview/chapter9/9-c.html [↑](#footnote-ref-38)
38. Mattel Inc v. Walking Mountain Productions, No. 01-56695 (9th Cir. Dec 29, 2003). http://archive.ca9.uscourts.gov/ca9/newopinions.nsf/6205C146C29519CC88256E0B005D8100/$file/0156695.pdf

    ^ Art ROGERS v. Jeff KOONS; Sonnabend Gallery, Inc., 960 F.2d 301 (2d Cir. Apr 2, 1992). http://bulk.resource.org/courts.gov/c/F2/960/960.F2d.301.91-7396.91-7540.91-7442.234.235.html [↑](#footnote-ref-39)
39. <https://www.eff.org/issues/intellectual-property/guide-to-youtube-removals> and http://www.youtube.com/t/contentid [↑](#footnote-ref-40)
40. Universal City Studios v. Reimerdes, 111 F. Supp. 2d 294, 322 (S.D.N.Y. 2000) [↑](#footnote-ref-41)
41. See http://www.copyright.gov/1201/ [↑](#footnote-ref-42)
42. http://www.copyright.gov/fedreg/2012/77fr65260.pdf [↑](#footnote-ref-43)
43. DMCA Section 1201 [↑](#footnote-ref-44)
44. http://www.copyright.gov/fedreg/2012/77fr65260.pdf [↑](#footnote-ref-45)
45. http://www.realnetworks.com/press/releases/2008/090808\_realdvd.aspx [↑](#footnote-ref-46)
46. http://arstechnica.com/uncategorized/2008/09/real-dvd-legit-dvd-copying-playback-but-is-it-too-late/ [↑](#footnote-ref-47)
47. ibid [↑](#footnote-ref-48)
48. http://arstechnica.com/tech-policy/2009/08/realdvd-barred-from-market-while-judge-opines-about-fair-use/ [↑](#footnote-ref-49)
49. http://arstechnica.com/tech-policy/2007/11/the-insanity-and-genius-of-frances-anti-file-sharing-plan/ [↑](#footnote-ref-50)
50. ibid [↑](#footnote-ref-51)
51. ibid [↑](#footnote-ref-52)
52. http://arstechnica.com/tech-policy/2008/01/frances-plan-to-turn-isps-into-copyright-cops-on-track/ [↑](#footnote-ref-53)
53. http://papers.ssrn.com/sol3/papers.cfm?abstract\_id=1989240 [↑](#footnote-ref-54)
54. Ibid p 14 [↑](#footnote-ref-55)
55. Ibid p 14 [↑](#footnote-ref-56)
56. ibid p15 [↑](#footnote-ref-57)
57. Ibid p 16 [↑](#footnote-ref-58)
58. Ibid p16 [↑](#footnote-ref-59)
59. Ibid p 20 [↑](#footnote-ref-60)
60. http://digitalcommons.calpoly.edu/mgmt\_fac/7/ [↑](#footnote-ref-61)
61. Link to agreement itself [↑](#footnote-ref-62)
62. MOU Pg 8 [↑](#footnote-ref-63)
63. MOU Pg 8 [↑](#footnote-ref-64)
64. MOU Pg 3 [↑](#footnote-ref-65)
65. MOU Pg 3-4 [↑](#footnote-ref-66)
66. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2145059> pg 19 [↑](#footnote-ref-67)
67. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2145059> pg 19 [↑](#footnote-ref-68)
68. MOU Pg 4 [↑](#footnote-ref-69)
69. MOU Pg 5 [↑](#footnote-ref-70)
70. MOU Pg 6 [↑](#footnote-ref-71)
71. MOU Pg 4 [↑](#footnote-ref-72)
72. MOU Pg 7 [↑](#footnote-ref-73)
73. MOU Pg 8 [↑](#footnote-ref-74)
74. MOU Pg 8 [↑](#footnote-ref-75)
75. MOU Pg 11 [↑](#footnote-ref-76)
76. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2145059> pg 21 [↑](#footnote-ref-77)
77. MOU Pg 13 [↑](#footnote-ref-78)
78. MOU Pg 7 [↑](#footnote-ref-79)
79. MOU Pg 14 [↑](#footnote-ref-80)
80. MOU Pg 26 [↑](#footnote-ref-81)
81. MOU Pg 30 [↑](#footnote-ref-82)
82. MOU Pg 30 [↑](#footnote-ref-83)
83. MOU Pg 29 [↑](#footnote-ref-84)
84. MOU Pg 30 [↑](#footnote-ref-85)
85. MOU Pg 26-28 [↑](#footnote-ref-86)
86. MOU Pg 29 [↑](#footnote-ref-87)
87. MOU Page 30 and 31 [↑](#footnote-ref-88)
88. MOU Pg 33 [↑](#footnote-ref-89)
89. MOU Pg 35 [↑](#footnote-ref-90)
90. http://www.pcworld.com/article/255061/judge\_throws\_out\_mass\_john\_doe\_porn\_copyright\_lawsuits.html [↑](#footnote-ref-91)
91. http://arstechnica.com/tech-policy/2009/07/o-tenenbaum-riaa-wins-675000-or-22500-per-song/ [↑](#footnote-ref-92)
92. http://arstechnica.com/tech-policy/2007/03/students-largely-ignore-riaa-instant-settlement-offers/ [↑](#footnote-ref-93)
93. http://www.techdirt.com/articles/20100713/17400810200.shtml [↑](#footnote-ref-94)
94. ibid [↑](#footnote-ref-95)
95. ibid [↑](#footnote-ref-96)
96. http://arstechnica.com/tech-policy/2008/12/no-more-lawsuits-isps-to-work-with-riaa-cut-off-p2p-users/ [↑](#footnote-ref-97)
97. http://arstechnica.com/tech-policy/2009/07/o-tenenbaum-riaa-wins-675000-or-22500-per-song/ [↑](#footnote-ref-98)
98. ibid [↑](#footnote-ref-99)
99. https://mywebspace.wisc.edu/mwbourgeois/web/06-cv-1497/336-1.pdf [↑](#footnote-ref-100)
100. http://arstechnica.com/tech-policy/2012/09/minnesota-file-sharer-loses-appeal-must-pay-222000/ [↑](#footnote-ref-101)
101. http://arstechnica.com/tech-policy/2012/05/finnish-court-rules-open-wifi-network-owner-not-liable-for-infringement/ [↑](#footnote-ref-102)
102. https://www.eff.org/deeplinks/2011/08/open-wifi-and-copyright-liability-setting-record [↑](#footnote-ref-103)
103. ibid [↑](#footnote-ref-104)
104. ibid [↑](#footnote-ref-105)
105. “It is well-established that the lawful owner of a copyright cannot infringe its own copyright.” Olan Mills, Inc. v. Linn Photo Co., 23 F.3d 1345, 1348 (8th Cir. 1994) [↑](#footnote-ref-106)
106. http://beckermanlegal.com/Lawyer\_Copyright\_Internet\_Law/virgin\_thomas\_080924Decision.pdf [↑](#footnote-ref-107)
107. http://arstechnica.com/tech-policy/2012/11/influential-gop-group-releases-shockingly-sensible-copyright-memo/ [↑](#footnote-ref-108)
108. http://arstechnica.com/tech-policy/2012/04/judge-rejects-copyright-trolls-bittorrent-conscopyright infringement-theory/ [↑](#footnote-ref-109)
109. ibid [↑](#footnote-ref-110)
110. http://arstechnica.com/tech-policy/2011/02/random-defendant-outlawyers-p2p-attorney-gets-lawsuit-tossed/ [↑](#footnote-ref-111)
111. http://lauren.vortex.com/archive/000337.html [↑](#footnote-ref-112)
112. http://www.perftech.com/ [↑](#footnote-ref-113)
113. expand [↑](#footnote-ref-114)
114. http://arstechnica.com/uncategorized/2007/10/comcast-traffic-blocking-even-more-apps-groupware-clients-affected/ [↑](#footnote-ref-115)
115. http://www.npr.org/templates/story/story.php?storyId=4989260 [↑](#footnote-ref-116)
116. http://blogs.technet.com/b/markrussinovich/archive/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far.aspx [↑](#footnote-ref-117)
117. http://arstechnica.com/information-technology/2010/07/court-breaking-drm-for-a-fair-use-is-legal/ [↑](#footnote-ref-118)
118. ibid [↑](#footnote-ref-119)
119. <http://www.ca5.uscourts.gov/opinions/pub/08/08-10521-CV0.wpd.pdf> p3 [↑](#footnote-ref-120)
120. <http://www.ca5.uscourts.gov/opinions/pub/08/08-10521-CV0.wpd.pdf> pg 7 [↑](#footnote-ref-121)