
PEER-TO-PEER (P2P) TECHNOLOGY: LEGAL AND POLICY CHALLENGES

INFOSYS 296A-2, SPRING 2005

UNIVERSITY OF CALIFORNIA AT BERKELEY

BENJAMIN HILL

UC BERKELEY SCHOOL OF INFORMATION

REPORT 2009-033 PUBLISHED JUNE 2007

ABSTRACT

Legislative protection that provides for a fair and balanced market of copyrighted material becomes much more challenging as new technology including peer-to-peer file sharing (P2P) reduces the transaction costs of obtaining copyrighted material. This paper examines the current state of P2P trading and technology in relation to the currently applicable laws, and makes proposals on how the existing laws could be modified to better adapt to the rapidly changing forefront of technology. These laws will lose much of their relevance as P2P technology approaches what I call the “P2P Singularity” of completely anonymous file exchange, where identification and prosecution of infringing individual users becomes technically infeasible. At this point, the majority of the laws protecting digital copyrighted material lose much of their relevance as the cost and ability to enforce the laws becomes drastically higher than the overall benefit gained. After the networks have evolved to this point, this paper examines several of the new business models that copyright owners could adopt in order to continue to profit.

Keywords: P2P, Peer-to-peer, File sharing, legal, copyright, anonymous, darknet

Neither individuals nor corporations have any right to come into court and ask that the clock of history be stopped, or turned back, for their private benefit.¹

P2P'S CURRENT STATE

While posing a significant threat to the existing revenue model of the music and motion picture industry associations, collectively the "P2P," participating in current P2P technology is a highly exposed activity. As evidenced by the more than 5000 lawsuits that the RIAA has initiated against individual high-volume infringers, individual sharing of music and movies online is a visible activity. The RIAA has been able to identify individual traders of copyrighted music, track and log their trading activities, collect sufficient evidence to initiate John Doe lawsuits against traders, and successfully subpoena individual identities from ISPs. The most popular programs, including Bittorrent, Gnutella-based networks, and eDonkey-based networks, all make no claims as to any anonymizing features of the technology. While some existing networks, including Freenet, are constructed to optimize anonymity, the lack of rapid search and slow file transfer as thus far prevented their widespread adoption. Current P2P networks are also vulnerable to a variety of technical techniques to raise the transaction costs of obtaining content, giving rise to an entire industry-for-hire of causing damage to P2P network communities. "Network Poisoning," or introducing garbled or fake versions of popular tracks into a network, is a common technique used to frustrate downloaders of music. It is unknown but feasible that the music industry would employ methods of monitoring and/or disruption the larger structure of P2P networks. Even without intentional disruption, existing P2P networks suffer from difficulties of searching, finding, and downloading music that is currently inherent to the fully decentralized nature of post- Napster P2P applications. The growing amount of clients behind firewalls or NATs decreases overall contribution to the network while increasing the drain on network resources. Anecdotally, the time required to download a movie over a standard connection is still longer than the amount of time it takes the author to bike to the local DVD rental store.

GOALS OF AN OPTIONAL SOLUTION

An optional solution to the P2P "Challenge" would be a legal structure that continues to protect the rights of copyright holders and optimizing the overall industry revenue, while at the same time protecting technical and market innovations including new forms of P2P technology. For the capital investment of building a music distribution infrastructure, identifying artists, promoting the music, and acting a "venture capitalist" of music, the music industry deserves to have enough protection to have a chance at continuing to make a profit within the existing market. With P2P networks introducing means of acquiring the industry's product at near transaction free levels, an appropriate amount of legal production becomes necessary. Civil penalties should be set at a level that provides a strong disincentive to infringe on copyrighted material while remaining proportional to the actual amount of harm an individual can cause. At the same time, technological innovations have time and time again proven to create new markets, sometimes far greater than the market that was originally threatened by the innovation. An ideal solution to providing legal protection to copyright holders would continue to allow innovation, only allowing the existing industry to challenge a business's use of technology, not the underlying technology itself.

RECOMMENDED MODIFICATIONS TO EXISTING LAW

For individuals that commit copyright violations, the existing system of penalties is far out of proportion to the amount of harm a single sharer of MP3 files actually causes to the music industry. It is evident that the large financial penalties for copyright infringement are designed to punish the individual who shared the files taking into

¹ ROBERT A. HEINLEIN, LIFE-LINE (1939)

consideration that the files will then be re-shared to others. The disproportionately large fine-per-violation is also designed to act as a public deterrent, allowing the music industry's media campaigns to play up the huge financial amount that P2P users risk losing if they are caught trading music online. I argue that the fines are far out of proportion to the actual damage that a single individual causes.

When committing copyright infringement of a song, or "stealing" it as the music industry likes to phrase it, industry has lost out on the amount that the user downloading the music would have had to pay for the music, times the percentage chance that the user would have bought the music had the P2P transaction costs been higher than purchasing the music directly. Furthermore, the user is then again liable for whatever level of contributory infringement is deemed appropriate given that they offered the file again to others for download. Given this total is often for hundreds of thousands of dollars under copyright law, it seems much more appropriate to fine users the average amount that the RIAA is settling for with the John Doe lawsuits – in the range of a few thousand dollars. In effect, the amount of fines is self-regulating, with the RIAA setting a more appropriate level of fines through their own willingness to settle for far less than the law currently allows. Keeping the "nuclear" option of the RIAA being able to sue for the full amount under the law is an unreasonable measure of liability against people that share music online – the entire network is causing millions of dollars in damage, but that is due almost entirely to the network effect. One individual sharing music online would not be a threat to the music business without the network. The fines still need to be significantly more than the cost to the user of purchasing the music directly, or there would be no risk to "stealing" the music and users would download freely, purchasing the music if (or when) they were identified.

The question of contributory infringement, one of the main issues in the MGM vs. Grokster case, is more difficult to find a balance between promoting the science and arts through copyright protection, while promoting technological innovation through protection from lawsuits from copyright holders. This paper proposes a modification to the method of determining if a technology is capable of "Significant Non-Infringing Uses." (SNIU) A technology, in itself, cannot be held as a "evil" technology by design. Time and time again, what initially appeared to be a huge threat against the existing music or movie industry has turned into the next major source of revenue, and it is yet unknown if P2P will follow the same trend. Instead, an optional construction of the law would allow a company's business model built around a technology to be sued as being reliant on contributory infringement. If in the court's opinion, the business model in use would not be viable if the copyrighted material was "magically" completely removed from the network, then the business is responsible for contributory infringement and can be sued for damages accordingly. Note that this makes no commitment as to if removing the copyrighted material is technically feasible, and it would be in each case a decision left to the court as to if the business could stand on its own if the copyrighted material suddenly vanished. This is directly in line with the Supreme Court questioning of "In other words, are they building their business on supporting legitimate activity, or, instead, are they building their business supporting infringing activity?"²

Simpler than the test of business model sustainability is determining if the marketing or advertising used to build the volume of a network encourages infringing activity. It should already be clear to the courts as to if a P2P network builds its membership base through marketing to infringing uses. The difference between "download music" and "download the latest Metallica" is very clear-cut, and should not present a challenge for the courts to legislate appropriately.

² METRO-GOLDWYN-MAYER STUDIOS, INC. v. GROKSTER, LTD, ET AL. No. 04-480 (2005) p. 10 line 2

Taken together, these modifications to existing civil penalties protecting copyright holders from infringing users on P2P networks should continue to afford protection to copyright holders in the short term. However, these protections are at best a legal band-aid, as this paper will investigate.

UNADVISABLE OPTIONS

The courts and congress may choose to protect the AA's investment in the current content distribution structure in a variety of ways not recommended by this paper, many of which have the potential for severely negative consequences. The courts may choose to restrict the development of infringing technologies in a variety of ways, including holding inventors responsible for developing the software used in P2P networks, responsible for developing anonymizing features as methods used to avoid detection, failure to build in appropriate anti-infringement filters, and responsible for the distribution of the client software programs. Software and hardware used to circumvent DRM technology is currently considered illegal as part the Digital Millennium Copyright Act (DMCA) passed in 1998, an extremely slippery slope when used to prevent fair-use copying of protected content. Mandating DRM technology into common electronic devices before DRM has been given a chance to become "consumer friendly" may end up creating more backlash that protection gained.

The courts may also continue to allow the copyright holding associations to push up the level of penalties, as well as creating criminal penalties for infringement, in an attempt to use heavily publicized immense levels of fines to scare off consumers from copying protected material. One such example is the recent Family Entertainment and Copyright Act, currently approved by congress, which would provide for up to three years jail time for distributing a single copy of a pre-release movie online. The author believes that it should never be the goal of the courts to punish one individual for another's actions, and basing the an individual's level of fines on how much downstream copying of a single shared media file might undergo is making one person pay for the actions of the entire network.

There is also the option of increasing the tax on storage media to compensate for the amount lost to piracy. Already in some countries the iPod is 1/3rd cheaper than in the USA due to the heavy tax imposed on MP3 capable devices to offset the theoretical losses due to copyright infringement. Arguably, this tax punishes everyone because of a few people's infringing activities and would be extremely difficult to "give back" to the artists that are losing money through infringing activities without the monitoring, tracking, and control of the major corporations. Placing a tax on the hardware legitimizes the copying of content and helps to consolidate control into the grip of a few major corporations, in turn creating barriers against the development and viability of new business models.

Alternately, "throwing open the floodgates" and determining that the owners of P2P networks have no contributory liability, allowing the network developers and owners to profit directly off of copyright infringement, would in itself be a form of contributory infringement by the courts. Individual liability is unlikely to be suddenly rendered obsolete by the courts; persons who commit large-scale copyright infringing activities will continue to face civil penalties. As such, giving free reign for P2P network operators to advertise their services as a 'great way to steal music' invites a infringement on a massive scale while at the same time setting individuals up for being sued by the RIAA. A similar argument applies to the other links in the P2P network technology stack, including restricting ISPs from advertising faster bandwidth as a good way to download illegally obtained movies.

Holding developers of technology responsible for the potential infringing uses of the technology is highly unadvisable. Similar to the concern of the Supreme Court in *MGM vs. Grokster*, the protection of the hypothetical garage iPod inventor, and promoting the development of technology through copyright protection the promotion of innovation, is paramount to the overall health of the economy. Examining an extreme case, the development and deployment of an anonymous and encrypted communication services could theoretically be used to promote

free speech in nations with an oppressive government, much as the initial goal of the Freenet system purports to do.³

THE P2P “SINGULARITY”

When creating laws regarding technology, it is important to structure the laws in such a way that they are flexible enough to remain relevant as technology continues to rapidly evolve. In order to determine if any proposed solution for legislating or regulating P2P technology is flexible enough to last, the logical evolution of the technology following a Moore’s law-like exponential improvement curve must be balanced against the capability of the legislation to continue to provide relevant levels of enforcement. The current generation of P2P networks is constrained by a variety of factors, including level of anonymity, media compression, ease of search, vulnerability to poisoning, and client bandwidth. Assuming that all of these factors will continue to improve at an exponential rate, the theoretical limit of a “final-generation” P2P network will be completely anonymous, fully encrypted, using highly compressed media files that are difficult to poison, easily searchable, all of which is connected through client bandwidth of a high enough capacity as to make the acquisition of new media including music, games, and movies nearly instantaneous. At this point the entire P2P network becomes a unified Darknet, impenetrable to the eyes of the RIAA/MPAA attempting to identify copyright infringing users. In this theoretical limit case of P2P networks, all that would be visible to an observer is a steady stream of encrypted communication passing between computers. Any content downloaded by a user would be through proxies, further increasing the anonymity of the network.⁴ This paper argues that this fully anonymous and encrypted P2P network could be considered a “singularity” in that the network itself could be used to mask the original creators and maintainers of the network, releasing updates to the software through the network itself. Once such a network has been achieved, nothing short of limiting end user bandwidth or completely blocking of encrypted communication could bring it down.

Many of the main-stream P2P networks currently have a single point of dependency that the legal system can focus its efforts against. In the case of Napster, the central server and the legally vulnerable corporation were the same entity. In the case of Grokster, while the network was distributed, there still existed a legally targetable company that contributed software updates and maintained the network. In the case of the hypothetical “final-generation” network, there would be no visible single entity profiting from the improvements and extension of the network. An anonymous coder could be the one releasing the software, hidden behind the very network he or she helps to create. Under this case, there is no structure or corporation directly benefiting from the network, and as such, no detectable contributory infringement.

Within the thought experiment of this “final-generation” P2P network, the cost of enforcing copyright law far outstrips the value gained from enforcing said laws. Legislative solutions to the P2P issue at this point become a moot point, and users that choose to trade in infringing works become free to do so with impunity. The author proposes that this potential “expiration date” for any law aimed at reducing copy infringement should be constructed with these approaching limitations in mind.

PUSHING BACK THE SINGULARITY

The RIAA and congress have both legal and technical methods that could be used to forestall the mass infringement that such a network would provide. A recent development is promoting a software program to concerned parents that searches their family computer for potentially infringing content, and either deleting the

³ Overview of Freenet’s goals at <http://encyclopedia.lockergnome.com/s/b/Freenet>

⁴ No longer theoretical since 2002: See “Tor: An anonymous Internet communication system” at <http://tor.eff.org/>

content located or reporting to the parent on the results. This model is likely to be merged with the “Rental Car Black Box” model insurance model, where a renter can either choose to have their speed monitored by a black box and receive a discounted rate, or choose to be unmonitored and pay a premium rate. There are multiple potential financial and legal incentives the RIAA could use to introduce similar black box monitoring techniques into the home PC, such as software bundled with ISP connectivity and built in hardware-level DRM. In the theoretical case of the ISP mandatory software install, both the ISP and the copyright owners have an incentive to reduce the bandwidth usage of the consumer. There may be other similar mutually beneficial partners that the RIAA and MPAA could use to bundle DRM protection with, and in every case, it will be up to the consumer market to either reject the technology with built in limitations⁵ or to accept the constraints imposed by the copyright owners.⁶

Unfortunately, some uses of P2P technology go well beyond that of copyright infringement. The most publicized examples is the trading of child pornography through anonymous P2P networks, or exchanging terrorist information. The FBI is continually investigating methods of monitoring and locating individuals exchanging this type of illegal information as the criminals continue to use ever more sophisticated means of encrypting and disguising their actions. The increase in easily used anonymizing technology in P2P networks will make it more common for criminals to share this type of material with less fear of reprisal. However, attempting to legislate the technology by framing it in the worst possible use would eventually lead to the removal of all privacy on any forms of communication. This argument quickly devolves into the same “we cannot let fear remove our right to privacy” debate on personal freedoms vs. government imposed monitoring, one that is outside the scope of this paper.

Raising the transaction cost of P2P downloading may be the recording industry’s best bet to convert individuals over to online purchasing of music. Poisoning the network through the introduction of scrambled or misleading files can raise the user’s frustration level with obtaining free music. The networks are also vulnerable to attack, including methods used to fragment or flood distributed networks. It would not be surprising to this author if congress grants copyright owners the right to attempt this sort of network poisoning against P2P networks that are not based in a corporate entity.

BEYOND THE HORIZON: NEW BUSINESS MODELS

Eventually, enforcement of copyright in a digital world will become more costly than the content being protected. Given that the cost of copyright enforcement will continue to rise until it becomes infeasible to locate and prosecute individuals, legal protection, if any, would revert to prosecuting the network owners. However, in the case of the proposed “final-generation” network, there may not be a corporate entity profiting from the network, and the developers may be hiding behind the very network they created. In this case, the “New Business Models” of making a profit in the era of technically unenforceable copyright protection (or “content is free”) will necessarily become a significant factor.

It remains to be seen if the “new business models” are viable in scope similar to the distribution infrastructure created by the music and movie industries. Many of the various new business models proposed center around making a profit off of the customer relationship while giving away the content. This technique has yet to have a market impact that is visible to the average consumer. The entry costs of the content is free new business models are, by definition, almost negligible, which would imply that struggling bands would attempt the new models before or in lieu of the traditional music industry contract model. Through established distribution methods such

⁵ See Sony’s struggling line of proprietary music format portables, and their eventual shift back to MP3 compatible players. http://news.com.com/Sony+to+support+MP3/2100-1027_3-5377625.html

⁶ iTunes being a leading example of consumer excepted DRM.

as Bittorrent, content can be distributed nearly cost free, yet if content producers were making money with the method, is there any reason we would have heard of the success? Perhaps by the very nature of the distribution and revenue model, the “small hit” family of bands making money off of transaction-free content distribution will never receive the level of press that the current model generates. Therefore, the new business models may already be working for some small bands, and until the press chooses to highlight success stories, the majority of consumers would be completely unaware of the new methods being tried. A possible factor is that people want to feel “with it” and listen to what the other cool people are listening to: without an overarching media mechanism promoting music, the cynic wonders how will people be told what they like? Other possibilities include an overt suppression of new business models by the RIAA. The music industry is continuing to make a significant profit distributing music through CDs, and has invested significant capital into storefronts and physical delivery mechanisms.

The new business model of artistic content distribution needs a modern proven case of an entity turning a significant profit while giving away the content. Once this band or movie studio successfully gambles on the new forms of revenue realization, and the free content model is acknowledged in the press as a viable business alternative, the RIAA and MPAA’s clock is ticking for the current industry leaders establishing a beachhead in the new marketplace. In the meantime there are already legal alternatives to P2P copyright infringement with little or no transaction costs, which may help smooth the transition to the new business model economy. iTunes allows friends on the same network to listen to your music, one song at a time, and without making a duplicate of the music file. The Mercore network is an advertising based streaming solution, which has paid the broadcasting fees for all of it’s members to broadcast songs to each other. Programs like StationRipper allow users to automatically record internet radio and podcast stations. All that remains is the establishment of a sustainable, proven revenue model.

CONCLUSION

The logical “final-generation” P2P network may not be technically feasible. It may be that searching and file transfer is too slow in a fully anonymous model, and that the current transparent file trading networks are as good as P2P will get. In this case, the business owners will continue to be liable in some respect, hopefully in a method similar to the SNIU modification listed previously in this paper. Individuals will continue to be sued for infringing activities, hopefully in an amount closer to the actual damage caused by the individual, instead of levying fines based on the network effect. This may be the state that the laws remain in as slow, small inroads are made into alternate content distribution. However, the author believes that once the major P2P networks “go dark” and anonymity and encryption become the rule instead of the norm within the space of P2P trading, the majority of the laws break down. At this point, the legal protection necessary to stop the infringing actions would be so damaging and intrusive to computing in general that it would become infeasible to legislate a solution. The RIAA may choose to partner with hardware, software, and service providers to install DRM to prevent infringement at the doorways to the P2P network, but within the network, content will be free.