"HANG 'EM HIGH"[1]: WILL THE RECORDING INDUSTRY ASSOCIATION OF AMERICA'S NEW PLAN TO POSSE UP WITH INTERNET SERVICE PROVIDERS IN THE FIGHT AGAINST ONLINE MUSIC PIRACY FINALLY TAME THE WILD INTERNET?

TABLE OF CONTENTS

[1] DOMINIC FRONTIERE, HANG 'EM HIGH (MCA Records 1968).

I. INTRODUCTION: "ONCE UPON A TIME IN THE WEST"[2]

> *Internet freedom isn't synonymous with a Wild West in which the taking of our property is accepted or, at best, ignored.*
>
> —*Mitch Bainwol*[3]

The prevalence of online music piracy has led some interested parties to characterize the Internet as a modern version of the Wild West: a place where brazen outlaws regularly abscond with millions of dollars worth of stolen music without fear of retribution. For five years the Recording Industry Association of America[4] (RIAA) attempted to combat that lawlessness by aggressively suing individuals suspected of illegally trading music files online.[5] However, in the wake of immense criticism over its methods,[6] and mounting evidence suggesting the futility of its efforts,[7] the RIAA has shifted strategies. On December 19, 2008, The Wall Street Journal reported the formation of agreements in principle between the RIAA and several major Internet service providers[8] (ISPs) under which the two traditionally adversarial parties will work together to combat online music piracy.[9]

---

[2] ENNIO MORRICONE, ONCE UPON A TIME IN THE WEST (RCA Records 1969).

[3] *The Internet Freedom Preservation Act of 2008: Hearing on H.R. 5353 Before the Subcomm. on Telecomm. and the Internet of the H. Comm. on Energy and Commerce*, 110th Cong. 3 (2008) (statement of Mitch Bainwol, Chairman and CEO, Recording Industry Association of America, on pending network neutrality legislation).

[4] The RIAA is the trade group that represents the recording labels that "create, manufacture and/or distribute approximately 90% of all legitimate sound recordings produced and sold in the United States." RIAA, Who We Are, http://www.riaa.com/aboutus.php (last visited Apr. 16, 2009).

[5] The RIAA initiated its litigation strategy against individuals on September 8th, 2003, and to date has sued over 30,000 individuals, including Durwood Pickle, a seventy-one-year-old grandfather, Brianna Lahara, a twelve-year-old girl living in public housing with her single mother, and—in one instance—a dead person. *See* Electronic Frontier Foundation, *RIAA v. The People: Four Years Later*, Aug. 2007, http://w2.eff.org/lP/P2P/riaa_at_four.pdf [hereinafter *RIAA v. The People*] (documenting the RIAA's recent litigation efforts). Lahara ultimately settled the case and was ordered to pay $2,000 and issue a public apology. *Id.*

[6] *See, e.g.*, *id.* ("There is no question that the RIAA's lawsuit campaign is unfairly singling out a few people for a disproportionate amount of punishment.").

[7] *See File-Sharing 'Not Cut by Courts,'* BBC NEWS, Jan. 20, 2006, http://news.bbc.co.uk/2/hi/entertainment/4627368.stm ("The level of file-sharing has remained the same for two years despite 20,000 legal cases in 17 countries.").

[8] An ISP is "an entity offering 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." Digital Millennium Copyright Act, 17 U.S.C. § 512(k) (2000).

[9] Sarah McBride & Ethan Smith, *Music Industry to Abandon Mass Suits*, WALL ST. J., Dec. 19, 2008, at B1.

Indeed, the prevalence of online music piracy has reached astounding proportions. Since 1999, the major recording labels[10] have lost forty-three percent of their business.[11] Record sales declined eleven percent from 2007 to 2008 alone.[12] Meanwhile, a survey of youths and their digital music collections found that the average teenager's digital music player contains more than 800 illegally obtained songs, and that nearly ninety-six percent of people between the ages of eighteen and twenty-four illegally copy music in some form.[13] These figures suggest that while the public is still consuming vast amounts of music, they are paying for far less of it.

The precipitous decline in record sales over the last eight years correlates with the rise in popularity of peer-to-peer[14] (P2P) file-sharing applications. Between the years 2000 and 2006, when record sales plummeted by almost two hundred million units,[15] online music piracy via P2P applications doubled.[16] These days, various forms of P2P file sharing account for between fifty and ninety percent of overall Internet traffic on the Web.[17] While the technology is capable of legal

---

[10] Collectively, Warner Music Group, EMI, Sony Music, and Universal Music Group (also known as the Big Four). Steve Jobs, *Thoughts on Music*, APPLE, Feb. 6, 2007, http://www.apple.com/hotnews/thoughtsonmusic/ (describing the role played by the "big four" in licensing arrangements).

[11] David Peisner, *No Money, Mo' Problems*, SPIN, Jan. 2009, at 72.

[12] NIELSEN SOUNDSCAN, STATE OF THE INDUSTRY 2007–2008, at 14 (2008), *available at* http://www.narm.com/2008Conv/StateoftheIndustury.pdf. Further, sales are expected to decline an additional nine percent over the next five years. Dawn C. Chmielewski, *Recording Labels and Websites in a Music Video Tussle*, L.A. TIMES, Dec. 23, 2008, at C1.

[13] Dan Sabbagh, *Average Teenager's iPod has 800 Illegal Music Tracks*, TIMES (London), June 16, 2008, at 13 (citing Michael Filby, *File-Sharers: Criminals, Civil Wrongdoers or the Saviours of the Entertainment Industry? A Research Study into Behaviour, Motivational Rationale & Legal Perception Relating to Cyber Piracy*, 5 HERTFORDSHIRE L.J. 2, 23 (2007), *available at* http://www.herts.ac.uk/fms/documents/schools/law/HLJ_V5I1_Filby.pdf (discussing the prevalence of and reasons for online digital piracy)).

[14] P2P applications "allow computer users to share electronic files . . . directly with each other, not through central servers." Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 919–20 (2005). Examples of popular P2P applications include Napster and Morpheus. *Id. passim*.

[15] Brian Hiatt & Evan Serpick, *The Record Industry's Decline*, ROLLING STONE, June 28, 2007, http://www.rollingstone.com/news/story/15137581/the_record_industrys_decline. This figure also includes digital sales of albums. *Id.* Specifically, the study found that albums declined from 785.1 million albums in the year 2000 to 588.2 million in the year 2006. *Id.*

[16] *See RIAA v. The People*, *supra* note 5. The data was for the years 2003 to 2005, with the number of simultaneous illegal downloads reaching a peak of 8.9 million in June of 2005. *Id.*

[17] Peter Svensson, *Comcast Blocks Some Internet Traffic*, WASH. POST, Oct. 19, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/10/19/AR2007101900842.html. *But see* Press Release, MultiMedia Intelligence, P2P Traffic to Grow Almost 400% over the Next 5 Years, as Legitimate P2P Applications Become Meaningful Segment (Oct. 21, 2008), *available at* http://www.

uses,[18] P2P applications facilitate the majority of online music piracy.[19] One study concluded that P2P usage "reduces the probability of buying music by an average of 30%," and that "without file sharing—sales in 2002 would have been around 7.8 percent higher."[20]

Of course, none of these statistics are news to the RIAA, which has targeted P2P applications for years. After alterations in P2P architecture forestalled suits against creators of P2P applications, the RIAA initiated an aggressive mass litigation strategy against users of those applications.[21] Five years and 35,000 suits later,[22] the RIAA now has all but abandoned that method of copyright enforcement in favor of a kinder, gentler strategy premised on the idea that warnings will provide the accountability necessary to curb online music piracy.[23]

---

multimediaintelligence.com/index.php?option=com_content&view=article&id=133:p2p-traffic-to-grow-almost-400-over-the-next-5-years-as-legitimate-p2p-applications-become-a-meaningful-segment&catid=37:frontpagetitleonly (estimating that 33.6% of North American Internet activity is P2P, while worldwide that number is 44%).

[18] *See* Nate Anderson, *Forecast: Legal P2P uses growing 10x faster than illegal ones*, ARS TECHNICA, Oct. 22, 2008, http://arstechnica.com/news.ars/post/20081022-forecast-legal-p2p-uses-growing-10x-faster-than-illegal-ones.html (noting that legal P2P traffic is growing ten times faster than illegal P2P traffic).

[19] *See* INTERNATIONAL FEDERATION OF THE PHONOGRAPHIC INDUSTRY, IFPI DIGITAL MUSIC REPORT 2008, at 19, *available at* http://www.ifpi.org/content/library/dmr2008.pdf ("P2P file-sharing still accounts for the large bulk of digital piracy.").

[20] Alejandro Zentner, *Measuring the Effect of File Sharing on Music Purchases*, 49 J.L. & ECON. 63, 66 (2006) (study representative of seven European countries). *But see* John Borland, *File-Sharing Has No Impact on CD Sales, Says Research*, SILICON.COM, Mar. 30, 2004, http://networks.silicon.com/webwatch/0,39024667,39119638,00.htm (arguing that online music piracy has no effect on declining CD sales).

[21] In 1999, the RIAA sued the P2P application Napster on theories of contributory and vicarious liability for the copyright infringing activity of its users. *See* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1010–11 (9th Cir. 2001). In that case and subsequent cases like it (*see, e.g.*, Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 940 (2005) (finding for entertainment industry against Grokster on theories of secondary liability)), the RIAA prevailed when the court determined a P2P hosting music files on a central server database accrues sufficient knowledge of the infringing activity to allow contributory and vicarious liability to attach. *Id.* at 1020. However, alterations in P2P architecture dispensing with central server databases complicated the issue of knowledge and forced the RIAA to litigate against P2P users directly. *See generally* Niva Elkin-Koren, *Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic*, 9 N.Y.U. J. LEGIS. & PUB. POL'Y 15, 17 (2006) (detailing the history of RIAA copyright enforcement efforts).

[22] *See* McBride & Smith, *supra* note 9.

[23] *See id.* (quoting Mitch Bainwol as suggesting that people are less likely to download illegally if they are "aware that their actions are not anonymous"). *See also* Karl Bode, *72% Of P2P Pirates Would Stop With ISP Warning*, DSL REPORTS, Oct. 13, 2008, http://www.broadbandreports.com/shownews/72-Of-P2P-Pirates-Would-Stop-With-ISP-Warning-98402 (finding evidence that illegal file-sharers would stop after receiving warnings from their ISP). The RIAA also might have been inspired to change direction due to a recent court decision. In one highly publicized case, a

Under the new plan, the RIAA will monitor the networks of the ISPs with which it has an agreement and notify them if it determines one of their customers is potentially sharing illegally downloaded music online.[24] The ISP will then either forward the notice to the customer, or alert the customer that he or she is suspected of illegally sharing music files and ask them to stop.[25] If users believe they are being targeted erroneously, they may challenge their status by administrative appeal to the ISP.[26] However, if the appeal is unsuccessful and the customer refuses to stop engaging in what the RIAA and the ISP believes are illegal activities online, the ISP may intentionally degrade (i.e., slow down) the Internet traffic of that user[27] or altogether cancel the user's Internet subscription.[28] Finally, though the RIAA is significantly reducing its litigation against individuals, it reserves the right to sue particularly egregious or stubborn copyright violators.[29]

For ISPs, the rise of P2P usage has been both a blessing and a curse. While the increase in popularity of P2P applications has been cited as a major impetus behind the exponential growth of the Internet and demand for high-speed connections offered by ISPs, these applications also consume large portions of network bandwidth, congest networks, and slow down Internet activity for other users.[30] ISPs would like to manage their networks to avoid the congestion resulting from increased P2P use, while not alienating some of their customers by

---

defendant who was ordered to pay $220,000 in damages to various recording labels won a retrial, along with a request by the judge for Congress to rethink damage awards in such cases. *See* Capitol Records Inc. v. Thomas, 579 F. Supp. 2d 1210, 1227 (D. Minn. 2008) (imploring Congress to address and reform the liability and damages issues in P2P cases so as to avoid gratuitous damages, thus potentially reducing the amount of money the RIAA can win in such cases).

[24] McBride & Smith, *supra* note 9.

[25] *Id.* The warning process is repeated as many as two additional times. *Id.*

[26] *See* David Kravets, *No ISP Filtering Under New RIAA Copyright Strategy*, WIRED, Dec. 19, 2008, *available at* http://blog.wired.com/27bstroke6/2008/12/no-isp-filterin.html (quoting RIAA spokeswoman Cara Duckworth that a system would be created that allowed accused users to challenge the violations).

[27] McBride & Smith, *supra* note 9.

[28] *Id. But cf.* Paul Resnikoff, *Any There There? RIAA Agreements Remain Flimsy, Unconfirmed . . .*, DIGITAL MUSIC NEWS, Jan. 4, 2009, http://www.digitalmusicnews.com/stories/122208riaa/?searchterm="any%20there%20there". Representatives from several ISPs—including AT&T, Road Runner, Verizon, and Earthlink—have denied that their respective employers will terminate their users' accounts. A representative from Verizon said it has resisted—and will continue to resist—any effort by the RIAA to perfect a "wholesale short-circuit of the legal system . . . in which alleged copyright holders are handled in bulk." *Id.* Other ISPs—such as AOL, Comcast, and Charter—did acknowledge the existence of agreements and furthermore their intentions to protect copyrighted material by terminating users' accounts. *Id.*

[29] McBride & Smith, *supra* note 9.

[30] *See* Elkin-Koren, *supra* note 21, at 18 (arguing that P2P use "boosted [ISP] business . . . but at the same time created a growing burden of limitless bandwidth consumption").

blocking access to their favorite applications.[31] The RIAA's new plan arguably offers ISPs the best of both worlds—the excuse to limit some P2P traffic on their networks, while not appearing to be actively doing so themselves. Meanwhile, the RIAA reaps the benefit of attacking online music piracy at its source: the gateway through which illegal file-sharers access the Internet.

However, numerous questions as to the new plan's legality and efficacy remain. This Note discusses whether the new plan will reduce online music piracy, and whether it will result in the discrimination of legal online content in contravention of recently espoused principles of network neutrality (NN).[32] Part II begins with an overview of how the RIAA identifies illegal file-sharers and introduces some of the problems it is likely to face in doing so. Next, Part II provides an overview of the Internet and describes how its unique architecture lends itself to use by P2P applications. Part II then discusses principles of NN and introduces the recent Federal Communications Commission's (FCC) decision against Comcast.[33] Finally, Part II presents the concept of voluntary collective licensing[34] (VCL) as an alternative to the new plan. Part III discusses the likelihood of the new plan's success given the potential pitfalls discussed in Part II. Specifically, this Part argues that the new plan—while an improvement over previous strategies—is not likely to achieve the RIAA's longtime goal of stopping online music piracy and taming the wild Internet, and that the RIAA should instead adopt a VCL scheme.

II. BACKGROUND: "FISTFUL OF DOLLARS"[35]

A. HOW THE RECORDING INDUSTRY ASSOCIATION OF AMERICA MONITORS PEER-TO-PEER TRAFFIC

Under its new plan, the RIAA—not ISPs—will search P2P applications for material sent online that potentially infringes a copyright of one of its member recording labels.[36] But in order to gauge the new plan's potential effectiveness, one must first understand how the RIAA analyzes Internet traffic.

---

[31] *See id.* at 67–68 (noting that P2P applications cause congestion of ISP's networks, but that P2P applications nevertheless attract customers).

[32] NN is discussed in detail in the Background portion of this Note, *infra* pp. 279–84.

[33] Free Press and Public Knowledge Against Comcast Corp., 23 F.C.C.R. 13028 (2008).

[34] VCL is discussed in detail in the Background portion of this Note, *infra* pp. 284–85.

[35] ENNIO MORRICONE, A FISTFUL OF DOLLARS (RCA Records 1967).

[36] *See* Kravets, *supra* note 26 (quoting Cara Duckworth, RIAA spokeswoman as saying, "There's no filtering [on the part of ISPs]. We are simply passing along a notice of detection and the ISPs will forward a notice to the subscriber."). One potential reason why ISPs are not actively monitoring their networks and instead allowing the RIAA to do so is because ISPs are immune to liability stemming from the infringing activities of their users only so long as they qualify for safe

1. Method of Monitoring. The RIAA hires companies like MediaSentry[37] and DtechNet[38] to monitor unlawful file sharing. These companies typically access P2P applications and search for the presence of songs whose distribution rights are owned by one of the RIAA's member organizations.[39] On LimeWire, a popular P2P application, a typical search for a copyrighted song can pull up hundreds of matches.[40] LimeWire allows users to right-click on a song entry and choose "browse host" to reveal all the songs a file-sharer has made available for others to download.[41] LimeWire also lists the IP addresses[42] of the user, which MediaSentry then uses to determine which ISP provides service to that user.[43] The above process is automated, enabling these entities to speedily check the online availability of thousands of songs.[44] After turning up matches by song name, these entities then use software to check the digital fingerprint of the file[45]

---

harbor under Title II of the Digital Millennium Copyright Act of 1998 (DMCA). *See* 17 U.S.C. § 512 (2000) (providing safe harbor for ISPs hosting infringing content if they comply with certain notice and takedown procedures). An ISP qualifying for safe harbor under § 512(a) remains in the safe harbor only so long as it acts as a neutral conduit of Internet traffic. Arguably, an ISP acts a neutral conduit under § 512(a) when it blindly transmits P2P content. *Id.* § 512(a). Therefore, the fact that the RIAA is analyzing content might mean that ISPs can remain in the safe harbor. However, some commentators argue that the safe harbor provisions might not apply to P2P applications. *See, e.g.*, Brian Yeh & Robin Jeweler, *Safe Harbor for Service Providers Under the Digital Millennium Copyright Act*, C.R.S. REP. No. RL32037 (2004), http://www.library.dau.mil/CRS_RL32037.pdf (describing the safe harbor regime of the DMCA and noting that recent court cases have held that certain types of service providers may not be subpoened under § 512(b) to identify P2P music file-sharers). Can ISPs remain in the safe harbor by allowing someone else to monitor their networks, or will their cooperation in the RIAA's new plan eject them from the safe harbor? This question—while interesting and relevant—is outside of the scope of this Note.

[37] MediaSentry is "a global provider of online content protection and promotion services for companies in the entertainment and software industries." MediaSentry.com, Company Overview, http://www.mediasentry.com/corp/overview/index.html (last visited Apr. 16, 2009).

[38] DtecNet.com, Our Solutions, http://dtecnet.com/EN/Our%20Soloutions/Anti-Piracy.aspx (last visited Mar. 3, 2009) ("DtecNet software solutions cover . . . online tracking of illegally distributed files.").

[39] *See* Catherine Rampell, *How It Does It: The RIAA Explains How It Catches Alleged Music Pirates*, CHRON. HIGHER EDUC., May 13, 2008, *available at* http://chronicle.com/free/2008/05/2821n.htm (describing the RIAA's monitoring scheme). In January 2009 the RIAA terminated its relationship with MediaSentry and announced its intention to solely employ DtecNet in a similar capacity. *See* Sarah McBride, *Changing Tack, RIAA Ditches MediaSentry*, WALL ST. J., Jan. 5, 2009, at B2 (detailing the RIAA's recent decision to terminate its contract with MediaSentry).

[40] Rampell, *supra* note 39.

[41] *Id.*

[42] *Id.* ("An IP address is a unique number, assigned by Internet-service providers, that identifies every connection to the Internet.").

[43] *Id.*

[44] *Id.*

[45] One way in which DtecNet can check the digital fingerprint of a packet is to look for the

to determine if it is identical to the copyrighted song.[46] Under the new plan, the RIAA then contacts the ISP, which then forwards a warning to the suspected file-sharer.[47]

However, legal challenges exist to this method of enforcement. For one, it is easier for an entity like DtecNet to determine a user is making a copyrighted song available for download than it is to determine the song has actually been illegally distributed.[48] In several recent court cases, judges have rejected the "making available" standard, and instead insisted the RIAA demonstrate "actual distribution" to prevail in lawsuits against suspected illegal file-sharers.[49]

---

presence of digital rights management (DRM) files on the transmitted file. DRM refers to "the use of technological tools used by copyright owners and distributors to regulate the uses of their works, and in particular to restrict reproduction." Rob Frieden, Internet Packet Sniffing and Its Impact on the Network Neutrality Debate and the Balance of Power Between Intellectual Property Creators and Consumers 6 n.14 (Aug. 16, 2007) (unpublished manuscript, *available at* http://works.bepress.com/robert_frieden/2/ (follow "Download the Paper" hyperlink)). However, DRM might be falling by the wayside. On January 2, 2009, Apple announced its intention to remove DRM software from the songs it sells in its online music store, iTunes. *See generally* Brad Stone, *Want to Copy iTunes Music? Go Ahead, Apple Says*, N.Y. TIMES, Jan. 6, 2009, at B1 (describing Apple's plans to drop DRM). All of the major recording labels have agreed to remove DRM from their songs. *Id.* Commentators applauded the move, and many argue that DRM alienated customers by restricting their use of the songs they purchase, while doing little to nothing to slow online music piracy. *Id.*

[46] Rampell, *supra* note 39. If this software does not definitively detect a match, then MediaSentry engages in other processes—including downloading and listening to the song in question—to determine if it matches a copyrighted song. *Id.* At this point in the RIAA's previous litigation strategy, it would initiate suit against individuals using their IP addresses and eventually sue the ISPs that provide Internet access to those users to obtain the users' names and addresses. *See generally RIAA v. The People*, *supra* note 5.

[47] McBride & Smith, *supra* note 9.

[48] *See The Future of Video: Challenges in Promoting Competition and Protecting Intellectual Property: Testimony Before the Federal Communications Commission En Banc Hearing on Broadband and the Digital Future*, 110th Cong. 1 (2008) (statement of Jon M. Peha, Carnegie Mellon University), *available at* http://www.fcc.gov/broadband_digital_future/072108/peha.pdf [hereinafter *The Future of Video*] (describing the problems associated with analyzing content online).

[49] *See* Capitol Records Inc. v. Thomas, 579 F. Supp. 2d 1210, 1218–19 (D. Minn. 2008) (rejecting the making available standard for copyright infringement and instead requiring showing of actual distribution of illegally uploaded songs for liability to attach); *see also* Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1162 (9th Cir. 2007) (affirming actual distribution standard); Atl. Recording Corp. v. Brennan, 534 F. Supp. 2d 278, 281–82 (D. Conn. 2008) (affirming actual distribution standard). *But see* Elektra v. Barker, 551 F. Supp. 2d 234, 244 n.8 (S.D.N.Y. 2008) (noting that making copyright works available *might* constitute a violation of the distribution right if further distribution was contemplated).

Further, in *Lava Records v. Amurao*,[50] MediaSentry's role in identifying allegedly illegal file-sharers on P2P applications was called into question.[51] In *Lava*, the defendant argued that testimony from MediaSentry tending to show illegal file sharing should be excluded because MediaSentry was operating as a private investigator without the proper state licensure.[52] However, the case against the defendant might not go to trial because the RIAA moved to dismiss the case with prejudice.[53] Whether or not entities like MediaSentry or DtecNet need an investigator's license to undergo their inspections is as yet undetermined.[54]

Also, some commentators believe this method of identification could lead to cases of mistaken identity.[55] For example, it is possible for a user to deliberately obfuscate his identity online, or make it appear he is actually another user.[56] Additionally, "where IP addresses change dynamically, it may be possible to identify the IP address of a violator correctly, but get the timing wrong and then map this IP address to the wrong individual."[57] These cases of mistaken identity potentially raise serious evidentiary issues should the RIAA initiate suit against a suspected file-sharer.

Once P2P users know the RIAA is analyzing material being sent over ISPs' networks, they can engage in certain countermeasures to prevent or hinder detection. Users can encrypt shared files, or scrub them in an effort to remove digital fingerprints. Encryption technology conceals the contents of transfers, making it difficult if not impossible to distinguish legal from illegal exchanges through traditional methods.[58] While not widely used, encryption technology is

---

[50] Memorandum of Law in Support of Motion to Exclude Testimony at 1–2, Lava Records v. Amurao, No. 7:07-CV-00321 (S.D.N.Y. Jan. 28, 2008), *available at* http://www.groklaw.net/pdf/MotExclMediaSentry.pdf (arguing that any evidence compiled by MediaSentry is inadmissible because it was compiled in absence of the relevant state investigative licensure).

[51] *See generally* Eric Bangeman, *MediaSentry Role in RIAA Lawsuit Comes under Scrutiny*, ARS TECHNICA, Feb. 3, 2008, http://arstechnica.com/tech-policy/news/2008/02/mediasentry-role-in-riaa-lawsuit-comes-under-scrutiny.ars (describing the problems MediaSentry has encountered).

[52] Lava Memorandum, *supra* note 50.

[53] Bangeman, *supra* note 51.

[54] Several states have laws requiring licensures of such entities. *See* Eric Bangeman, *Michigan Says MediaSentry Lacks Necessary PI License*, ARS TECHNICA, Mar. 11, 2008, http://arstechnica.com/tech-policy/news/2008/03/michigan-says-mediasentry-lacks-necessary-pi-license.ars [hereinafter *Michigan*] (finding similar laws requiring state private investigator licensure for entities like MediaSentry in Michigan, Massachusetts, and Oregon).

[55] *See The Future of Video*, *supra* note 48, at 4 (noting that limitations in existing technology might contribute to cases of misidentification).

[56] *See id.* (noting that while it is theoretically possible for a user to deliberately obscure his or her true identity, or make it appear as though he or she is actually another user, "this hypothetical problem has not been proven to exist, or disproven").

[57] *Id.*

[58] *Id.*

readily available in some of the leading P2P applications, and is likely to become more widespread once P2P users begin receiving warnings from their ISPs.[59] As Apple CEO Steve Jobs said, "[T]here are many smart people in the world, some with a lot of time on their hands, who love to discover such secrets and publish a way for everyone to get free (and stolen) music."[60] Engaging in the type of analysis necessary to inspect encrypted music files might inspire more sophisticated encryption techniques and initiate a war of attrition between entities like DtecNet and the individuals described by Steve Jobs.

2. Fair Use, Fairly Complicated. Finally, even if the RIAA identifies material it believes infringes a copyright, it must be wary of fair use issues. Fair use falls under section 107 of the Copyright Act[61] and provides for "a reasonable and limited use of a copyrighted work without the author's permission."[62] While fair use does not provide carte blanche for users to distribute copyrighted music to one another, there are nevertheless instances where one user might be operating within the purview of fair use when he sends an otherwise copyrighted song to another user over a P2P application.

The doctrine of fair use protects the reproduction, public distribution, and any other use of an otherwise copyright protected song specified in 17 U.S.C. § 106 "for purposes such as criticism, comment, news reporting, teaching . . . scholarship, or research."[63] A fair use analysis contemplates several factors, including the purpose and character of the use, the nature of the copyrighted work, the amount and substantiality of the portion used in relation to the whole, and the effect of the use on the potential market for the copyrighted work.[64] So long as a given use falls under one of these categories, the use is protected and is not an infringement of copyright.[65] The doctrine of fair use is a balancing of interests between promoting the progress of science and useful arts under the

---

[59] *Id.* ("[I]f DPI were used in conjunction with some sort of punishment for those caught transferring copyrighted material, many users would probably turn encryption on.").

[60] Jobs, *supra* note 10. For a great example of the ingenuity of hackers, see Miles Raymer, *Let's Share: Not Even Music Execs Still Think They Can Stop Piracy*, CHI. READER, Feb. 23, 2007, http://www.chicagoreader.com/features/stories/sharpdarts/070223/ (chronicling several successful efforts of individuals to circumvent DRM technology).

[61] 17 U.S.C. § 107 (2000).

[62] BLACK'S LAW DICTIONARY 634 (8th ed. 2004).

[63] 17 U.S.C. § 107.

[64] *Id.*

[65] *Id.*

Constitution[66] and encouraging the creation of works for the public.[67] In this respect, fair use is "an equitable rule of reason that permits courts to avoid rigid application of the copyright statute."[68] The Supreme Court has denied the presence of bright-line rules in making fair use analyses, and instead called for a case-by-case analysis.[69]

While the RIAA makes the initial determination as to whether a user has potentially infringed a copyright, the ISP must be certain the user has infringed a copyright and is not within fair use before it acts to either slow down or terminate that user's account. At best, the monitoring system described above can determine whether copyrighted material is being transferred, but it cannot determine whether the individual involved in the transfer has the right to make the transfer in accordance with fair use. If the ISP does discriminate against legal P2P content, then it risks penalty by the FCC or potential legislation codifying NN principles, as described in Part III.

B. PRINCIPLES OF NETWORK NEUTRALITY AND THEIR EFFECT ON MONITORING EFFORTS

After the RIAA identifies a user it believes is illegally sharing files, it relies on the ISP to warn that user and potentially either slow down or terminate his account. However, ISPs must remain wary of NN, i.e., the principle that data packets on the Internet should be "moved impartially, without regard to content, destination, or source."[70] Potentially, NN prohibits ISPs from either slowing down or blocking the legal traffic of Internet users. In carrying through their portion of the new plan, ISPs run the risk of accidentally blocking legal Internet traffic and offending principles of NN.[71] Generally, ISPs oppose NN, while content

---

[66] U.S. CONST. art. I, § 8, cl. 8 (declaring Congress's power to "promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries").

[67] *See generally* 18 AM. JUR. 2D *Copyright and Literary Property* § 78 (2008) (describing the parameters of the doctrine of fair use).

[68] *Id.*

[69] *See* Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 577 (1994) (holding that the commercial purpose of petitioner's song did not prevent it from falling under the fair use doctrine).

[70] SearchNetworking.com Definitions, *Network neutrality*, http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci1207194,00.html (last visited Apr. 16, 2009).

[71] Press Release, Federal Communications Commission, FCC Adopts Policy Statement (Aug. 5, 2005), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-260435A1.pdf (announcing intention to "preserve and promote the open and interconnected nature of public Internet" by protecting legal online activities and applications).

providers are in favor of it.[72] This section describes NN and discusses recent attempts to enforce and even codify NN principles.

1. The Internet and Peer-to-Peer Technology. One cannot fully understand the genesis and implications of the NN debate without first understanding the architecture of the Internet. The Internet is comprised of intelligent end-user computers connected by an infrastructure, i.e., a network.[73] Internet communication occurs when a source computer at the edge of the network splits data into smaller units called packets and then submits those packets into the infrastructure of the network.[74] Besides content, the packets also carry basic information such as addresses of source and destination computers.[75] A series of routers read that basic information and transmit packets to successive routers until they reach their destination.[76]

Currently, end-users provide content for the Internet, meaning they are responsible for creating and posting Web pages and creating applications that others use to animate their Internet experiences. The debate over NN has been characterized as a fight over control of the Internet, with proponents of NN lobbying to keep control in the hands of end-users, and opponents of NN arguing for moving control to the center of the network and into the hands of the ISPs.[77] If ISPs do gain control of the Internet, they could theoretically control content as well as determine which applications can be used on their networks.

NN would also prevent ISPs from creating tiered levels of service based on content. Usually, each packet is routed along an ISP's network to its final destination without regard to content and without experiencing much delay.[78] However, a problem occurs when too many packets are sent at the same time, thus flooding the routers whose job it is to forward the packets along to the next destination.[79] Routers typically handle packets on a first-in, first-out basis.[80] But because bandwidth is limited, during periods of high traffic a router faces a

---

[72] JONATHAN D. HART, INTERNET LAW: A FIELD GUIDE 2006, at 750 (2006).

[73] *See* Edward W. Felten, Nuts and Bolts of Network Neutrality 1–2 (July 6, 2006) (unpublished manuscript, *available at* http://itpolicy.princeton.edu/pub/neutrality.pdf) (providing an overview of NN).

[74] Kai Zhu, Note, *Bringing Neutrality to Network Neutrality*, 22 BERKELEY TECH. L.J. 615, 616–17 (2007).

[75] *Id.*

[76] *Id.* at 617.

[77] *See* Felten, *supra* note 73, at 2 (describing in general the fight to control innovation on the Internet).

[78] *See id.* at 2–5 (describing in general the relative fluidity with which packets are sent through the network in periods of low traffic).

[79] Zhu, *supra* note 74, at 617–18.

[80] Felten, *supra* note 73, at 4.

"competition for limited resources" that may result in the need to queue incoming packets, which may in turn result in unpredictable delay in the transmission process, i.e., network congestion.[81]

In the early days of the Internet, network congestion was rarely a problem because most Internet users only checked e-mail or viewed Web pages, activities that require very little bandwidth.[82] However, the modern Internet is distinguished from the early days of the Internet by the increasing use of P2P applications. Because P2P applications are used to send large music or video files,[83] they require an amount of bandwidth disproportionate to the amount of people using P2P applications. The result is that a relatively small amount of people can dominate bandwidth and cause congestion that slows down the traffic of all other Internet users on a network.

ISPs could manage their networks by slowing down P2P traffic while privileging other kinds of traffic.[84] However, ISPs have a paradoxical relationship with P2P applications, because "[o]n the one hand, [P2P] programs increase the demand for high-speed access . . . [b]ut [P2P] programs also eat up space on a network," leaving providers "a clogged network [that] costs money and hurts their reputation."[85] ISPs therefore must walk a fine line in optimizing their networks to provide quality service to all of their customers, while not alienating the numerous customers who rely on high-speed Internet for their P2P applications. While reasonable network management during periods of high traffic is generally allowed, NN provides that ISPs cannot unreasonably discriminate against legal P2P applications in managing their networks.

2. Federal Communications Commission v. Comcast. In response to growing concern that ISPs might begin discriminating against applications and content providers on the Internet, the Federal Communications Commission (FCC) in February 2004 adopted a policy of "preserv[ing] and promot[ing] the open and interconnected nature of public Internet."[86] In its press release the FCC stated that

---

[81] Zhu, *supra* note 74, at 617–18.

[82] *See id.* at 618 (describing the growth of the Internet and the rise of bandwidth-eating applications).

[83] *See* Farhad Manjoo, *How Comcast Blocks Your Internet Traffic*, SALON, Oct. 19, 2007, http://machinist.salon.com/blog/2007/10/19/comcast.

[84] *See* Felten, *supra* note 73, at 2–5 (describing the methods by which ISPs could discriminate against certain kinds of Internet traffic in order to optimize their networks).

[85] Manjoo, *supra* note 83.

[86] FCC Press Release, *supra* note 71.

> (1) consumers are entitled to access the lawful Internet content of their choice; (2) consumers are entitled to run applications and services of their choice, subject to the needs of law enforcement; (3) consumers are entitled to connect their choice of legal devices that do not harm the network; and (4) consumers are entitled to competition among network providers, application and service providers, and content providers.[87]

The FCC's principles allow ISPs to reasonably manage their networks and discriminate against illegal content.

Detractors often label NN "a solution in search of a problem."[88] However, in 2007, a problem emerged. Robb Topolski is a fan of old-time barbershop quartet music, which he enjoys sharing with others over his Comcast Internet connection.[89] One day, when trying to share un-copyrighted music via a P2P network, Topolski discovered he was unable to upload any of his songs onto the network.[90] Concerned, Topolski drew upon his experience as a software tester and ran a protocol analyzer to determine exactly what was happening.[91] Topolski found, and subsequent tests by the Associated Press confirmed, that Comcast had engaged in an Internet traffic-management scheme in which they inspected packets to determine their content, and then intentionally interrupted packets containing P2P information.[92]

Soon after Topolski's revelation, public interest groups Free Press and Public Knowledge filed a Formal Complaint with the FCC, asking it to enforce the provisions of its Policy Statement protecting NN.[93] The Complaint alleged that "Comcast [was] secretly degrading innovative protocols used for transporting and sharing large files,"[94] and implored the FCC to "impose an immediate injunction and the maximum forfeitures" against them.[95] Among other violations, the

---

[87] *Id.*

[88] Anne Broache, *Tech Manufacturers Rally Against Net Neutrality*, CNET NEWS, Sept. 19, 2006, http://news.cnet.com/Tech-manufacturers-rally-against-Net-neutrality/2100-1028_3-6117241.html (quoting Rep. Bobby Rush (D-Ill.)).

[89] Robb Topolski's Journal, *My Opening Remarks to the FCC Today* . . . (Apr. 17, 2008, 20:38 EST), http://funchords.livejournal.com/195797.html.

[90] *Id.*

[91] Posting of Robb Topolski to DSL REPORTS, http://www.dslreports.com/forum/remark,18323368?hilite= (May 12, 2007, 14:26:36 EST).

[92] Manjoo, *supra* note 83.

[93] Complaint at i, Free Press and Public Knowledge Against Comcast Corp., 23 F.C.C.R. 13208 (2008) (No. 07-52), *available at* http://www.publicknowledge.org/pdf/fp_pk_comcast_complaint.pdf.

[94] *Id.*

[95] *Id.* at 12.

Complaint alleged that Comcast had prevented its customers from running applications and services of their choice, and accessing the lawful Internet content of their choice.[96] Comcast denied it was blocking any Internet application, and instead claimed it was reasonably delaying traffic during periods of network congestion.[97]

On August 1, 2008, in a Memorandum Opinion and Order, the FCC—in a narrow 3-2 decision—voted to enforce its NN principles and monitor Comcast's activity to ensure compliance with its order.[98] Specifically, the Opinion concluded that Comcast's "discriminatory . . . practice unduly squelches the dynamic benefits of an open and accessible Internet and does not constitute reasonable network management."[99] The Opinion stressed that Comcast's "failure to disclose [its] practice to its customers [had] compounded the harm."[100] The FCC maintained its distinction between legal and illegal content, extending NN protection only to the former.[101] While Comcast is challenging the ruling on the grounds that the FCC has no standing to enforce its policy statement,[102] the language in *National Cable v. Brand X* implies the FCC has leeway to impose additional regulatory requirements as it sees fit.[103]

3. Pending Network Neutrality Legislation. Besides the decision in *FCC v. Comcast*,[104] there currently is legislation pending to codify NN principles. On February 12, 2008, Rep. Edward Markey (D-Mass.) introduced House Bill 5353, the Internet Freedom Preservation Act (2008 Act).[105] The 2008 Act would amend Title I of the Communications Act of 1934[106] by adding a new section 12 to prevent unreasonable discrimination by ISPs, and to "preserve and promote the open and interconnected nature of broadband networks that enable consumers to

---

[96] *Id.* (alleging unreasonable network management on the part of Comcast).

[97] *See* Peter Svensson, *Comcast Admits Delaying Some Traffic*, MSNBC, Oct. 23, 2007, http://www.msnbc.msn.com/id/21444566/ (president of Comcast asserting that it "uses several network management technologies that, when necessary, enable us to delay—not block—some [P2P] traffic").

[98] Free Press and Public Knowledge Against Comcast Corp., 23 F.C.C.R. 13028 (2008).

[99] *Id.*

[100] *Id.*

[101] *Id.* at 13052.

[102] *See* Comcast Corp. v. Fed. Commc'n Comm'n, No. 08-1114, 2008 U.S. App. LEXIS 19067 (D.C. Cir. 2008).

[103] Nat'l Cable & Telecomm. Ass'n v. Brand X Internet Servs., 545 U.S. 967, 969 (2005) (indicating the FCC can impose additional regulation, requirements if it so chooses).

[104] *See supra* Part II.B.*2*.

[105] Internet Freedom Preservation Act of 2008, H.R. 5353, 110th Cong. (2008) (Act to codify principles of NN).

[106] 47 U.S.C. § 151 (1934).

reach . . . lawful content, applications, and services of their choosing."[107] Generally the language of the 2008 Act tracks the language of the FCC's NN policy statement.[108] Should the legislature pass the 2008 Act,[109] any questions raised by Comcast regarding the FCC's ability to enforce its policy statement would be moot, and claims for violations of NN would be brought under this 2008 Act instead of through the FCC.

C. POSSIBLE ALTERNATIVE: VOLUNTARY COLLECTIVE LICENSING

One alternative to the RIAA's new enforcement scheme is a voluntary collective licensing (VCL) scheme. VCL is distinguished from compulsory licensing[110] in that the recording industry and ISPs would enter into the agreement willingly, thus minimizing governmental intervention and letting market forces dictate the terms of the agreements.[111] VCL is supported by several Internet and music policy organizations, such as the Electronic Frontier Foundation.[112]

VCL operates under the premises that artists and copyright holders deserve fair compensation and that file sharing is a permanent fixture in the modern Internet landscape.[113] Under a VCL scheme, the music industry would create collection societies that would offer Internet users the opportunity to eschew illegal file-sharing in favor of making reasonably low monthly payments (e.g., ten dollars a

---

[107] H.R. 5353 § 12.

[108] The Act would (1) maintain the freedom to use broadband telecommunications networks, including the Internet, without unreasonable interference from or discrimination by network operators; (2) enable the United States to preserve its global leadership in online commerce and technological innovation; (3) promote the open and interconnected nature of broadband networks that enable consumers to reach, and service providers to offer, content, applications, and services of their choosing; and (4) guard against unreasonable discriminatory favoritism for, or degradation of, content by network operators based upon its source, ownership, or destination on the Internet. *Id.* The bill is currently in committee.

[109] Passage of the 2008 Act is far from a foregone conclusion. Since 2006, there have been six other attempts by Congress to codify principles of NN. For a summary of previous Congressional attempts to codify principles of NN, see Adam B. Summers, *Net Neutrality or Government Brutality?*, FREEMAN, July 1, 2008.

[110] A compulsory license is "a statutorily created license that allows certain parties to use copyrighted material without the explicit permission of the copyright owner in exchange for a specified royalty." BLACK'S LAW DICTIONARY 938 (8th ed. 2004).

[111] *See generally* Electronic Frontier Foundation, *A Better Way Forward: Voluntary Collective Licensing of Music File Sharing*, Apr. 2008, http://www.eff.org/wp/better-way-forward-voluntary-collective-licensing-music-file-sharing [hereinafter *A Better Way Forward*] (arguing for the institution of a voluntary collective licensing scheme).

[112] *Id.*

[113] *Id.*

month) for unlimited music downloads.[114] The collected money would then be divided among the various copyright holders based on the popularity of their music.[115] ISPs would bundle the fee into the price of their services.[116] Although there are numerous drawbacks and obstacles to such a solution,[117] some of the benefits are that artists would receive more money, the RIAA would avoid waging a technology war against hackers, and the everyday activities of millions of people around the world would be decriminalized.[118]

III. ANALYSIS: "HIGH NOON"[119]

Under its new plan, the RIAA will analyze P2P traffic and identify users illegally sharing copyrighted music. But how will the RIAA's methods of identification fare when dealing with file encryption and various other digital subterfuges? How will the RIAA know if a user is illegally sharing a copyrighted file, or whether he or she is sharing a copyrighted file pursuant to the fair use doctrine? Further, in carrying out their obligations under the new plan, how can ISPs be sure they are only discriminating against illegal content for purposes of complying with NN? Do the provisions of the new plan requiring them to slow down or terminate the accounts of users the RIAA believes are engaged in illegal file-sharing online qualify as reasonable network management under *Free Press and Public Knowledge Against Comcast Corp.*?[120]

In answering these questions, this Analysis first addresses the difficulties—practical and legal—of shifting through voluminous amounts of material online given encryption technologies as well as fair use issues. After discussing the pitfalls awaiting the RIAA, and the probable lack of success under the new plan, this section argues the RIAA should instead adopt a VCL scheme as a means for dealing with online music piracy. Secondly, this Analysis discusses whether ISPs can fulfill their obligations under the new plan without unintentionally discriminating against legal content online and therefore violating NN. This section concludes that the RIAA and ISPs should lobby for NN legislation that permits good faith discrimination against P2P content to avoid future sanctions from the FCC.

---

[114] *Id.*
[115] *Id.*
[116] *Id.*
[117] The drawbacks and obstacles will be discussed in detail in the Analysis portion of this Note, *infra* pp. 293–95.
[118] *A Better Way Forward*, *supra* note 111.
[119] DIMITRI TIOMKIN, HIGH NOON (RCA Records 1952).
[120] Free Press and Public Knowledge Against Comcast Corp., 23 F.C.C.R. 13028 (2008).

A. PROBLEMS WITH MONITORING PEER-TO-PEER CONTENT

1. Sheer Volume, Encryption, and Other Measures. Sifting through P2P traffic on an ISP's network is no small task. Currently over 413 million people—roughly forty-five percent of the population in the Americas—have Internet access.[121] In the United States alone, over 60 million people use P2P applications.[122] Comcast boasts 14.9 million high-speed Internet customers.[123] While certainly not all of those customers employ P2P applications, these numbers suggest a great number of them do. If—as some critics suggest—the RIAA terminated its mass litigation strategy partly because of the expenses it incurred,[124] then the potential cost of the new plan hardly seems like an improvement given the amount of monitoring it requires.

Of course, the RIAA itself is not monitoring P2P traffic online. For that Herculean task it has hired DtecNet.[125] According to DtecNet's Web site, the company provides software that tracks illegally distributed files online.[126] However, even an automated process designed to quickly analyze packets would need to shift through voluminous amounts of material continuously being sent across the network. While an automated service theoretically could handle the task, it is unclear how such a system would handle packets that have been encrypted or otherwise "scrubbed" so as to obfuscate their illegal freight. Some studies suggest that users can engage in a type of subterfuge in which their own illegal actions are attributed to another user.[127] These cases of mistaken identity—should they occur—could potentially embarrass the RIAA as well as complicate subsequent litigation against suspected file-sharers.

Once P2P users realize their activity is being monitored, they will probably engage in various countermeasures designed to frustrate detection by DtecNet.[128] If users do engage in encryption measures, DtecNet faces a significantly tougher task identifying illegal file-sharers. Theoretically, any automated process would require constant alterations in order to effectively monitor encrypted files (and

---

[121] InternetWorldStats.com, Internet Usage Statistics for the Americas, http://www.internetworldstats.com/stats2.htm (last visited Apr. 16, 2009).

[122] Electronic Frontier Foundation, *File Sharing*, http://www.eff.org/issues/file-sharing (last visited Apr. 15, 2009) [hereinafter *File Sharing*].

[123] Comcast, Corporate Overview, http://www.comcast.com/corporate/about/pressroom/corporateoverview/corporateoverview.html (last visited Apr. 16, 2009) (describing the Comcast Corporation).

[124] *See RIAA v. The People*, *supra* note 5.

[125] *See supra* note 39 and accompanying text.

[126] *See supra* note 38 and accompanying text.

[127] *See supra* notes 55–57 and accompanying text.

[128] *See supra* notes 58–60 and accompanying text.

arguably some encryption methods might entirely frustrate any such attempts). The additional work required might cost the RIAA and its member labels enough money to eviscerate any semblance of cost effectiveness under the new plan.

Further, in *Capitol Records* the judge asked Congress to consider amending the Copyright Act to reduce the amount of damages available to the RIAA in suits against alleged illegal file-sharers.[129] If Congress does amend the Copyright Act, or judges or juries consistently award the least amount of damages possible, then the RIAA will not be able to collect as much money from the egregious file-sharers it decides to sue. With the recording industry losing so much money anyway, the combination of these factors—expensive monitoring systems and less payout from litigation—might spell the demise of the new plan.

Aside from sheer volume and encryption, DtecNet might not be able to provide the RIAA with the kind of evidence it needs to prevail at trial against illegal file-sharers. Besides criticizing the damage awards in illegal file-sharing cases, the judge in *Capitol Records* also granted the defendant a retrial on the grounds that the RIAA needed to demonstrate actual distribution of copyrighted songs, not just that the defendant made the songs available for download.[130] DtecNet would need to ensure their investigation methods produce the kind of evidence the RIAA would need to prevail at trial. However, to overcome this evidentiary hurdle, *Capitol Records* holds that entities like DtecNet could simply download a copy of the song, thus demonstrating actual distribution.[131]

Finally, it is unclear whether—subsequent to recent challenges like the one in *Lava Records*[132]—entities such as DtecNet must obtain licensures to practice as investigators. Massachusetts, Michigan, New York and Oregon are examples of states that have recently called into question the ability of entities such as DtecNet to work as investigators absent the relevant state licensures.[133] While it is likely that DtecNet or other similar entities easily could obtain such licensures, as well as alter their detection methods in order to provide evidence of actual distribution, these are merely examples of the kinds of hurdles the RIAA is likely to face in prosecuting its plan.

2. Over-Enforcement of Copyright and the Problem of Fair Use. Even if the RIAA—through DtecNet—can account for encryption methods and other digital subterfuge, there is no automated process that can determine whether or not the

---

[129] *See supra* note 23 and accompanying text.

[130] *See supra* note 49 and accompanying text.

[131] *See* Capitol Records Inc. v. Thomas, 579 F. Supp. 2d 1210, 1216 (D. Minn. 2008) (the Eighth Circuit "holds that distribution to [a private investigator acting as an agent of the copyright holder] can form the basis of an infringement claim").

[132] *See supra* notes 50–52 and accompanying text.

[133] *See supra* note 54 and accompanying text.

fair use doctrine applies. The court in *Campbell* called for a case-by-case analysis to determine if fair use attaches in a given situation.[134] A case-by-cases analysis is the definitional antithesis of an automated process. The fair use doctrine demands a fact-intensive inquiry accounting for a variety of factors understandable only in reference to the circumstances in a given case.

Suppose a documentary filmmaker wants to send a clip of his movie over the Internet to a friend. Suppose further the clip contains a scene in which a brief snippet of a copyright protected song plays in the background. Under most applications, fair use probably would attach: the use is for a documentary, it is brief, and—for argument's sake—it is not the centerpiece of the given scene or film as a whole. Under the new plan, however, such uses probably would be identified as illegal and turned over to the ISP. Though an appeals process might absolve any erroneous warnings, the need to file an appeal might alienate some users, who might then flock to other ISPs with whom the RIAA does not have an agreement, thus further undermining the plan.

Further, the inability of the RIAA to distinguish fair use—as well as its inability to fully make any definitive determination as to illegality of a given transfer—probably will lead to over-enforcement of copyright. The RIAA has an incentive to identify as many illegal file-sharers as possible. In its haste, it probably will err on the side of warning a user if its initial investigation suggests the user is engaging in piracy. While the administrative appeals process is helpful, at some point ISPs—before slowing down or terminating an account—would have to conduct their own investigations into the allegedly infringing conduct, including making an informal determination as to whether fair use applies.

However, while the RIAA potentially saves money by turning in suspected illegal file-sharers, ISPs potentially lose money by terminating those users' accounts.[135] Therefore it seems likely an ISP will err on the side of caution in such a situation and not slow down or terminate its users' accounts absent an admission of guilt coupled with continued malfeasance, or near incontrovertible evidence of illegal conduct.

On the other hand, according to the RIAA, its new plan is premised on the idea that file-sharers will conform to the law if they know they will be held accountable for illegally sharing music online.[136] If all the RIAA wants to achieve is letting users know someone is looking over their shoulder, and if it believes that such behavior will discourage would-be file-sharers from engaging in illegal acts,

---

[134] *See supra* note 69 and accompanying text.

[135] This is notwithstanding any secondary benefit they receive by purging another bandwidth-hog from their congested networks.

[136] *See supra* note 23 and accompanying text.

then perhaps it is not necessary for ISPs to actually slow down or terminate the accounts of their users. While it would be nice if the mere threat of punishment—even if no actual punishment occurs—permanently forestalls illegal behavior, given the popularity of P2P applications, it seems very much like wishful thinking.

B. PROBLEMS WITH DISCRIMINATING AGAINST PEER-TO-PEER CONTENT

1. Checking It Twice: Engaging in Another Packet Analysis. The above sections demonstrate some of the problems associated with monitoring P2P networks. However, a whole new set of problems emerges once ISPs endeavor to fulfill their end of the agreement. To reiterate, once the RIAA believes it has identified illegal uses, it sends a warning to the ISP, which the ISP then forwards to the user.[137] According to the tentative terms of the new plan, after three such warnings, the ISP will either slow down the traffic of the user, or terminate his account.[138] However, if the ISP does either slow down or cancel accounts, it must be careful not to violate principles of NN in doing so. According to principles of NN, ISPs cannot discriminate against legal content on the Web.[139]

To be sure, NN is barely more than a concept at this point. While generally there is NN on the Internet, there currently are no federal laws protecting it. However, the 2008 Act is currently pending in the House of Representatives. If it passes both houses of Congress and is signed into law, it would protect NN and provide for its enforcement.[140] But if the 2008 Act follows the trajectory of other similar attempts to codify NN principles,[141] then it will soon fall by the wayside. On the other hand, awareness of NN has grown recently, with policy organizations like the Future of Music Coalition engaging in education campaigns stressing its importance.[142] Further, if ISPs like Comcast continue to engage in unreasonable network management, such behavior might engender more public and Congressional support for the 2008 Act.

Pending legislation notwithstanding, the FCC enforced its policy statement regarding NN in its decision against Comcast.[143] In that case, the FCC determined

---

[137] *See supra* notes 24–25 and accompanying text.

[138] *See supra* notes 27–28 and accompanying text.

[139] FCC Press Release, *supra* note 71.

[140] *See supra* notes 105–09 and accompanying text.

[141] *See supra* note 109 and accompanying text.

[142] *See, e.g.*, Future of Music Coalition, *Musicians Support Network Neutrality*, http://www.futureofmusic.org/rockthenet/ (last visited Apr. 16, 2009) (providing details for sale of a CD benefiting the future of Music Coalition's Rock the Net campaign for NN).

[143] Free Press and Public Knowledge Against Comcast Corp., 23 F.C.C.R. 13028 (2008).

that Comcast's traffic management scheme was unreasonable because it did not distinguish between legal and illegal content, and because it was done in secret.[144] If the appeals court follows *National Cable*, it probably will affirm the FCC's decision, and thus provide a mechanism for individuals to challenge traffic management schemes.[145]

The problem ISPs will face in discriminating against content identified by the RIAA is that their actions might violate NN as recognized by the FCC. After receiving warnings, the new plan provides users an opportunity to challenge the RIAA's allegations of online music piracy.[146] Presumably, during this process users will be able to deny the allegations, either outright or by reference to fair use or other theories. If after the administrative appeals process the ISP still believes the user illegally shared music files, it will slow down or terminate that user's account.[147] So long as the user did in fact illegally share music files, ISPs will not have violated NN. However, if one of the investigative entities made a mistake and the content was in fact shared legally, then ISPs might have violated NN by discriminating against legal content.

As noted above, the process of determining whether content is legal or illegal can be complicated by encryption and other digital subterfuge.[148] If the ISP takes its appeals process seriously, it will in effect have to re-analyze the evidence to determine whether the content sent actually was sent illegally. Therefore ISPs will need to proceed with caution to avoid accidentally discriminating against legal content.

While ISPs have an incentive to manage their networks to avoid congestion, they do not desire to alienate their customers.[149] Users who access P2P applications have fueled the need for high-speed Internet, which has put money in the ISPs' pockets.[150] ISPs probably do not want to terminate the accounts of some of their best users. Additionally, they do not want to risk violating NN and raising the ire of the FCC. Further, if the ISPs do discriminate against P2P content without engaging in due diligence first, they risk actually encouraging NN legislation. As noted above, it is already difficult for a court to determine if a use is fair under the Copyright Act. Therefore, when faced with these tough decisions as to whether a user is illegally sharing files or not, ISPs should err on the side of

---

[144] *Id.* at 13052–53, 13058–59.
[145] *See supra* note 103 and accompanying text.
[146] *See supra* note 26 and accompanying text.
[147] *See supra* notes 27–28 and accompanying text.
[148] *See supra* notes 55–60 and accompanying text.
[149] Elkin-Koren, *supra* note 21, at 67.
[150] *Id.* at 68.

extreme caution, slowing down or terminating the accounts of only the most egregious and obvious illegal music sharers.

2. Will Discrimination Qualify as Reasonable Network Management? On the other hand, the decision in *Free Press and Public Knowledge Against Comcast Corp.* only proscribes unreasonable network management.[151] Therefore, the relevant question becomes whether an ISP is engaging in reasonable network management when it acts in compliance with a request by the RIAA to slow down or remove the account of a user suspected of illegally sharing music, even if its initial determination of illegality turns out to be erroneous. Of course, the appeals process again becomes a relevant part of the equation.

In *Free Press*, the FCC held that Comcast's "discriminatory . . . practice unduly squelches the dynamic benefits of an open and accessible Internet and does not constitute reasonable network management."[152] The Opinion stressed that Comcast's "failure to disclose [its] practice to its customers [had] compounded the harm."[153] The Opinion—like FCC's policy statement and pending NN legislation—does not protect illegal content. For the purposes of the Opinion, if content is actually illegal, ISPs are acting well within their rights to remove it.

In many ways, the traffic management scheme under the new plan can be distinguished from the unreasonable traffic management in *Free Press*. In *Free Press*, the ISP was itself analyzing traffic and then discriminating against it, whereas in the new plan the RIAA is analyzing traffic and then alerting the ISP, which only slows down or terminates the account after an administrative appeals process. In *Free Press*, no effort was made to distinguish between legal and illegal content, whereas under the new plan the user can appeal her status as an illegal file-sharer.

It seems self-evident that discriminating against illegal content qualifies as reasonable network management. However, if an ISP acts in good faith based on evidence provided to it, but nevertheless mistakenly discriminates against the legal Internet activity of one user, those actions also might qualify as reasonable network management: reasonable because illegal content deserves no protection, and ISPs should be allowed—after investigation and an appeals process—to discriminate against a user's account.[154]

In *Free Press*, the FCC suggested that Comcast's secrecy in discriminating against certain users buttressed the finding of unreasonable network management.[155] ISPs under the new plan would likely avoid this problem as long

---

[151] Free Press and Public Knowledge Against Comcast Corp., 23 F.C.C.R. 13028 (2008).

[152] *Id.*

[153] *Id.*

[154] Whether or not such actions potentially violate due process is beyond the scope of this Note.

[155] *Free Press*, 23 F.C.C.R. at 13058–59 ("A hallmark of whether something is reasonable is whether a provider is willing to disclose to its customers what it is doing.").

as the user knows he is being investigated before his traffic is discriminated against. Further, ISPs could easily avoid secretive behavior by fully disclosing the terms of their agreement with the RIAA, something they have not done as of yet.[156] Though the FCC demands transparency as to the network management schemes of ISPs,[157] it seems like this is a standard ISPs could easily meet by simply informing their users of their plan to cooperate with the RIAA, as well as informing them of the methods by which this cooperation will occur.

Even if an ISP's activities under the new plan qualify as reasonable network management, it would behoove ISPs to push for alterations in the FCC's policy statement, or alterations in pending legislation, to permit good faith discrimination against content they believe is illegal. If the FCC declares that reasonable network management permits ISPs to—after an appeals process—discriminate in good faith against what they believe is illegal content on their network, even if later it turns out that the content is legal, then ISPs probably would not violate NN in carrying out their end of the new plan.

On the other hand, several ISPs have made it known they would like to manage their networks in ways that are not permitted under current iterations of NN. Therefore, it seems likely that the FCC and Congress would be particularly sensitive to discrimination that might be pretextual. As noted earlier, the RIAA has an incentive to over-enforce its copyrights. If ISPs are given carte blanche to discriminate against anything identified by the RIAA as potentially constituting illegal file-sharing, they could potentially discriminate against any content, even legal, under the guise of acting in good faith. To prevent such an eventuality from transpiring, the administrative appeals process must be rigorous, and users should be able to appeal to the FCC before their accounts are terminated.

3. Lobbying for Favorable Network Neutrality Legislation. Generally, ISPs oppose NN legislation.[158] NN legislation—at least as expressed in the 2008 Act—would prevent ISPs from discriminating against legal content.[159] ISPs generally oppose NN legislation because the ability to discriminate among content potentially could provide ISPs with a new source of income. They could conceivably charge more for Internet service for certain kinds of traffic. They could also privilege certain applications over others, which would enable them to strike deals with individual content providers. ISPs and the RIAA argue that the marketplace is a better mechanism for managing the Internet.

---

[156] *See* Resnikoff, *supra* note 28 (lamenting the paucity of details as to the specifics of many of the alleged agreements).

[157] *Free Press*, 23 F.C.C.R. at 13058 (criticizing Comcast's "failure to disclose its network management practices to its customers").

[158] HART, *supra* note 72.

[159] *See supra* notes 105–09 and accompanying text.

However, if such legislation gains the support that previous legislation has lacked, ISPs and the RIAA should lobby Congress to alter the Act to allow for exactly the kind of network management ISPs engage in when they fulfill their end of the bargain under the new plan. That is, ISPs should seek to have Congress recognize a good faith effort to distinguish between legal and illegal content online and discriminate against the illegal content in order to reduce online music piracy. ISPs should argue for declaring this kind of network management reasonable . That way, if they do wrongfully slow down or terminate a user's account, that user will have no basis to call for the FCC to levy sanctions against the ISP.

C. THE APPEAL OF VOLUNTARY COLLECTIVE LICENSING

Although some studies do suggest that many illegal file-sharers would stop if warned by the RIAA,[160] it is unclear whether those figures are accurate and whether they would hold up over time, particularly if encryption methods do surface which allow users to easily disguise their traffic. Further, the RIAA is experiencing more difficulty prosecuting the claims it does litigate. The new plan seems like a step in the right direction to the extent it focuses less on litigation, but given the problems described above, it probably is not the solution to the online music piracy problem.

Though there is no definitive solution to the piracy problem,[161] VCL schemes are appealing for a variety of reasons. Under VCL, the RIAA would not be battling the idle minds of thousands of computer hackers, all looking to make a name for themselves by discovering a way to frustrate DtecNet. Instead, users would be given the option of paying a monthly fee for the right to download as many songs as they can fit on their computers. While the plan still requires users to pay money—something they apparently have been hesitant to do—it allows them to do so in a lump sum attached to their Internet service bill. The file sharing they do subsequent to purchasing the service *feels* like it is free.

Perhaps more importantly, under a VCL scheme, artists and rights holders would receive money in proportion to the popularity of their music, a measurement determined by how often their music is downloaded. Because the RIAA currently works with the labels that produce ninety percent of all legitimate sound recordings in the United States,[162] they stand to benefit significantly from VCL. Further, their sales are likely to be more consistent, as users pay the fee

---

[160] *See supra* note 23 and accompanying text.

[161] *See* McBride & Smith, *supra* note 9 (Eric Garland, president of BigChampagne, a piracy consulting firm claiming "[t]here isn't any silver-bullet anti-piracy solution").

[162] *See supra* note 4 and accompanying text.

every month. Though users could drop and add VCL at any time, recording labels might benefit from knowing how much money they can expect to receive from VCL schemes, and plan accordingly and with more certainty.

Secondly, under a VCL scheme the market controls the terms of the agreement, and not the government, whose decisions—though arguably well-intentioned—are often hopelessly outdated by the time they are enacted. Some theorists argue that online music piracy is a problem because it was "not even a glimmer in anyone's eye when the DMCA was enacted."[163] If Congress does amend the Copyright Act, advancements in technology probably would render it obsolete fairly quickly. Conversely, under a VCL scheme, the parties—if they are committed to the concept—can alter the terms of the agreement as need be to account for changes in technology.

As for ISPs, theoretically they could make more money as the growing popularity of P2P applications—and the chance to use them legally—will inspire more people to purchase high-speed Internet.[164] Additionally, under a VCL scheme, ISPs would no longer need to worry about the RIAA finding a new way to file suit against them in a renewed effort to incorporate them into the fight against online music piracy.

On the other hand, a VCL scheme might further limit the role of the major recording labels in marketing music. VCL is extremely friendly to artists because they can plug into the VCL system and collect money directly from the collection societies, presumably without a major recording contract. Thus, the recording labels—who usually provide distribution of musicians' recordings—would be obsolete. However, the recording industry is losing money every year, and—as it currently still produces the majority of popular music in the country—it is likely it will embrace the short term solution, even if it drains them further down the road.[165]

VCL is but one alternative available to the music industry, and is an example of the kind of solution it would behoove the RIAA to consider implementing in its attempt to reduce online music piracy. While VCL is not a perfect solution to the problem, it would have the effect of decriminalizing the everyday activities of millions of Internet users worldwide, an act that would go a long way in earning back the trust of music lovers around the country.

---

[163] Brief for Alliance for Public Technology et al. as Amici Curiae Supporting Respondents, Recording Indus. Ass'n of Am. v. Verizon Internet Servs., Inc., 240 F. Supp. 2d 24 (D.C. Cir. 2003) (No. 1:02MS00323), 2002 WL 32387949 (arguing that the DMCA does not apply to P2P activity online).

[164] Elkin-Koren, *supra* note 21, at 65.

[165] Additionally, a VCL scheme might raise antitrust and accurate division of money issues, but these are beyond the scope of this Note.

IV. CONCLUSION: "HOW THE WEST WAS WON"[166]

Undoubtedly the music industry ain't what she used to be. The recording industry is scrambling to shore up its borders and repel the increasing wave of online music piracy. The RIAA's new plan represents a significant departure from the previous litigious methods that arguably produced little effect on online music piracy and alienated a generation of customers.

If its figures are accurate, then the RIAA's new warning system might make an appreciable difference in the short term.[167] However, it is unlikely that the new plan is the panacea the recording industry desires. For one, encryption methods and fair use issues make it difficult to distinguish legal from illegal content. If the RIAA engages in over-enforcement of copyright, then ISPs are likely to ignore the warnings or terminate their agreements with the RIAA. Additionally, if there are close issues as to fair use, then ISPs probably will err on the side of not terminating users' accounts. ISPs wish to avoid violating principles of NN. Though they do have an incentive to manage their networks, they are well aware that any unreasonable management might trigger penalties, or the very least encourage the passage of NN legislation.

Further, recent court cases indicate the RIAA is fighting an uphill battle in collecting money from illegal file-sharers. Not only have some recent cases forced the RIAA to prove actual distribution of copyrighted music,[168] but there are also some rumblings in the judicial system suggesting the amount of money recoverable in such actions should be significantly reduced.[169] Some recent cases have even called into question whether evidence compiled by entities like DtecNet is admissible.[170] If file-sharers are aware a suit brought by the RIAA against them does not immediately spell their demise, they are more likely to challenge the allegations in open court.

To be sure, online music piracy is a problem. Copyright holders and artists deserve fair compensation for the fruits of their labors. However, it seems unlikely that the new plan will drastically reduce online music piracy. Instead, the RIAA and ISPs should look into VCL schemes, which would allow millions of illegal file-sharers the opportunity to "get legit" by authorizing their ISP to charge them more per month in exchange for limitless downloads. Further, under a VCL scheme, artists and copyright holders could potentially receive more

---

[166] ALFRED NEWMAN, HOW THE WEST WAS WON (MCA Records 1963).

[167] *See* Bode, *supra* note 23 (noting new study indicating seventy-two percent of illegal downloaders would stop if warned by their ISP).

[168] *See supra* note 49 and accompanying text.

[169] *See supra* note 49 and accompanying text.

[170] *See supra* note 51 and accompanying text.

compensation, and the RIAA and other copyright holders could avoid the cost and headache of waging a technology war against hackers.[171]

Maybe it is not the Internet that is wild after all, but instead the RIAA's approaches to copyright enforcement. Though the RIAA's new plan is an improvement over its old one, it will probably not solve the online music piracy problem.

Not even Clint Eastwood could solve that one.

John Eric Seay

[171] *A Better Way Forward*, *supra* note 111.