THE JOHN MARSHALL
REVIEW OF INTELLECTUAL PROPERTY LAW

HOTFILE, MEGAUPLOAD, AND THE FUTURE OF COPYRIGHT ON THE INTERNET: WHAT CAN CYBERLOCKERS TELL US ABOUT DMCA REFORM?

ROSS DRATH

ABSTRACT

More than a decade ago, Napster brought the issue of copyright infringement by file-sharing to the center of the public stage. How would a body of copyright law built to regulate tangible objects apply in the digital realm? The safe harbor provisions of the Digital Millennium Copyright Act, intended as a compromise between the interests of copyright owners and webhosts, have instead introduced legal uncertainty and allocated the costs of online enforcement both inefficiently and disproportionately. While Napster and several other major peer-to-peer services have been shuttered in the intervening period, the scope of online copyright infringement continues to grow apace. One avenue of that growth has been the advent of a certain class of "cyberlockers"—file storage sites that incentivize and profit from mass infringement. Focusing on two particularly controversial cyberlockers, this comment analyzes the current state of copyright law on the Internet and suggests comprehensive, practical reforms with an aim to achieving a sustainable reduction in online infringement.

Cite as Ross Drath, *Hotfile, Megaupload, and the Future of Copyright on the Internet, What can Cyberlockers Tell us About DMCA Reform?*, 12 J. MARSHALL REV. INTELL. PROP. L. 205 (2012).

HOTFILE, MEGAUPLOAD, AND THE FUTURE OF COPYRIGHT ON THE INTERNET: WHAT CAN CYBERLOCKERS TELL US ABOUT DMCA REFORM?

ROSS DRATH

HOTFILE, MEGAUPLOAD, AND THE FUTURE OF COPYRIGHT ON THE INTERNET: WHAT CAN CYBERLOCKERS TELL US ABOUT DMCA REFORM?

ROSS DRATH*

INTRODUCTION

Think of your favorite movie. Now type that movie's name into a simple Internet search, adding the word "download" (you can even ignore your search engine's suggestion to include the word "free"). You are now practicing the most rudimentary, least efficient method of pirating a film; and yet, if you want to, you will *own* a digital copy of the movie—a product of countless man-hours and extensive investment—likely in less than an hour.[1]

File-sharing of copyrighted works exists in several forms. Over the past decade, popularity has shifted from peer-to-peer services like Limewire and Kazaa to BitTorrent sites like the Pirate Bay, and most recently to a certain class of cloud storage sites called "cyberlockers."[2] Though there is a dearth of reliable data regarding the scale of infringement-by-file-sharing, few honest observers argue that such activity occurs on a less than substantial basis.[3]

 J.D. Candidate, May 2013, The John Marshall Law School, Chicago, Illinois. B.A. in Philosophy, University of Michigan, Ann Arbor, Michigan. Many thanks to my friends and family for their invaluable support, encouragement, tolerance, and patience. Thanks also to the editorial staff of the John Marshall Review of Intellectual Property Law for its instrumental assistance in preparing this comment. Any errors are my own.

[1] *United States*, NETINDEX.COM, http://www.netindex.com/download/2,1/United-States/ (last visited Nov. 14, 2012) (reporting an average download speed of 15.36 megabits per second for U.S. users); *Physical Parameters*, MPEG.ORG, http://www.mpeg.org/MPEG/DVD/Book_A/Specs.html (last visited Oct. 31, 2012) (stating DVD capacity is 4.7 Gigabytes). While download speeds and file sizes will vary significantly, a 4.7 GB file would take approximately 43 minutes to download at a rate of 15.17 megabits per second.

[2] *See* Eriq Gardner, *Read the MPAA's Big Lawsuit Against 'Cyberlocking' Site Hotfile*, THE HOLLYWOOD REP. (Feb. 8, 2011, 12:04 PM), http://www.hollywoodreporter.com/blogs/thr-esq/read-mpaas-big-lawsuit-cyberlocking-97400 ("Cyberlockers are file-hosting websites whose stated purpose is to give users personal storage room for large files."). In a recent study, MarkMonitor, a brand security company, surveyed web-traffic data for sites dedicated to copyright and trademark infringement. MARKMONITOR, TRAFFIC REPORT: ONLINE PIRACY AND COUNTERFEITING (2011), *available at* https://www.markmonitor.com/download/report/MarkMonitor_-_Traffic_Report_110111.pdf. According to the study, the three most-visited digital piracy sites (rapidshare.com, megaupload.com, and megavideo.com) include two cyberlockers and a video streaming site that operates under the same brand name as one of those cyberlockers. *Id.* at 7; *see also Cyberlockers Take Over File-Sharing Lead from BitTorrent Sites*, TORRENTFREAK (Jan. 11, 2011), http://torrentfreak.com/cyberlockers-take-over-file-sharing-lead-from-bittorrent-sites-110111/ ("All signs indicate that file-storage services are becoming the new sharing standard.").

[3] *See* David G. Post, *SOPA and the Future of Internet Governance*, JUSTIA.COM (Feb. 13, 2012), http://verdict.justia.com/2012/02/13/sopa-and-the-future-of-internet-governance ("[N]obody can deny that there are an enormous number of [offshore websites offering copyrighted works for download], that many of them make a great deal of money by trampling on the legitimate rights of copyright and trademark owners, and that the consequent damage to those rights holders is substantial.").

In general, cloud storage sites provide substantial, legal cost benefits for consumers and service providers alike: Users receive a convenience benefit—they can access all the files they care to upload, anywhere and on any device with an internet connection; for their part, the proprietors of cloud storage sites maintain a consistent volume of use which they can translate into advertising and membership revenue. In recent years, the market for cloud storage has grown exponentially as more and more technology companies have come to recognize the value of this product.[4] The question is how to deter or devalue cloud services that are specifically designed to profit from infringement without impinging on non-infringing services.

The stated goal of Copyright Law is to produce public benefits by promoting progress in creative endeavors.[5] In the context of the Internet, "dual purpose" technologies (those that are capable of both infringing and non-infringing use) raise three competing public interests: (1) fostering authorship by protecting incentives to create, (2) promoting technological innovation, and (3) safeguarding free speech and the free flow of information.[6]

Parts I.A and I.B of this comment will trace the common law development of the doctrines of direct infringement and secondary liability as applied to online service providers. Part I.C will discuss the safe harbor provisions of the Digital Millennium Copyright Act (DMCA): how a webhost can qualify for safe harbor protection under the statute, and specifically how § 512(c) interacts with the secondary and direct liability doctrines to affect online webhosts' liability for users' acts of infringement.

Part III will examine the legal status of cyberlockers under that precedent, with particular attention to recent cases involving two major cyberlockers. Part IV surveys several solutions advanced by commentators and legislators, and proposes a set of significant changes to the existing scheme with the aim of establishing well-needed legal certainty and providing smart economic incentives to all parties involved. Part V sets forth a brief conclusion.

I. BACKGROUND

A. Direct Infringement

The Copyright Act of 1976 confers enumerated exclusive rights on the owner of a copyright.[7] Unauthorized use of copyrighted material, in violation of any of those

---

[4] *See* Press Release, Int'l Data Corp., Demand from Pub. Cloud Serv. Providers and Private Cloud Adopters Will Drive Strong Growth for Full Range of Storage Solutions, According to IDC (Oct. 20, 2011), http://www.idc.com/getdoc.jsp?containerId=prUS23097611 (estimating that "[b]y 2015, combined spending for public and private cloud storage will be $22.6 billion worldwide.").

[5] U.S. CONST. art. 1, § 8, cl. 8. ("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.").

[6] Jane Ginsburg, *Separating the Sony Sheep from the Grokster Goats: Reckoning the Future Business Plans of Copyright-Dependent Technology Entrepreneurs*, 50 ARIZ. L. REV. 577, 579 (2008).

[7] 17 U.S.C. § 106 (2012). The Act specifies six exclusive rights: reproduction, distribution, adaptation, public performance, public display, and, in the case of sound recordings, public performance by digital transmission. *Id.*

exclusive rights, constitutes infringement.[8] To prove direct copyright infringement, then, a plaintiff must show that she owns a valid copyright in the relevant work and that the alleged infringer copied that work in violation of one or more of the exclusive rights enumerated in § 106 of the Copyright Act.[9] Early on in the development of the Internet, one court held that the operator of a bulletin board service directly infringed copyrights in photographs that had been uploaded to the system independently by its subscribers.[10]

Since the 1995 decision in *Religious Technology Center v. Netcom, Inc.*,[11] however, the case law has quite clearly gone the other way. That is, most courts have adopted the view that, absent "volitional conduct" designed to cause infringement, online service providers do not directly infringe copyrights when their systems automatically and indifferently process users' upload and download requests.[12]

Commentators consider the *Netcom* framework to be fairly well established,[13] but in a narrow and parallel line of cases several courts have found its volitional requirement met by certain methods of system operation.[14] The touchstone in these cases seems to be human intervention. Most notably, in *Playboy v. Russ Hardenburgh*, the Northern District Court of Ohio held a system operator liable for direct infringement where its employees reviewed uploads before making them available for download.[15]

But in the *CoStar* case, in 2004, the Court of Appeals for the Fourth Circuit ruled the other way on similar facts, holding that employee review of user-posted material does not rise to the level of volitional conduct where the employees' conduct does not itself constitute infringement.[16]

---

[8] 17 U.S.C. § 501.

[9] *Id.*; *see also* Feist Pubs., Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 345–46 (1991).

[10] Playboy Enters., Inc. v. Frena, 839 F. Supp. 1552, 1559 (M.D. Fla. 1993).

[11] Religious Tech. Ctr. v. Netcom, Inc., 907 F. Supp. 1361 (N.D. Cal. 1995).

[12] *Id*. at 1369–70.

> Although some of the people using the machine may directly infringe copyrights, courts analyze the machine owner's liability under the rubric of contributory infringement, not direct infringement . . . . Although copyright is a strict liability statute, there should still be *some element of volition* or causation which is lacking where a defendant's system is merely used to create a copy by a third party.

Id.(emphasis added); *see also* Parker v. Google, Inc., 422 F. Supp. 2d 492, 497 (E.D. Pa. 2006) ("When an ISP automatically and temporarily stores data without human intervention so that the system can operate and transmit data to its users, the necessary element of volition is missing.").

[13] *See* 3 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 12B.01[A][1] (2012) [hereinafter NIMMER] (noting that Congress broadly endorsed the *Netcom* result in enacting the Digital Millennium Copyright Act); R. Anthony Reese, *The Relationship Between the ISP Safe Harbors and the Ordinary Rules of Copyright Liability*, 32 COLUM. J.L. & ARTS 427, 430–31 (2009) (reporting a trend in favor of the *Netcom* approach).

[14] *See* Playboy Enters., Inc. v. Webbworld, Inc., 991 F. Supp. 543, 552 (N.D. Tex. 1997) (distinguishing *Netcom* on the ground that the system operator altered the files and "took affirmative steps to cause the copies to be made"); Playboy Enters., Inc. v. Russ Hardenburgh, Inc., 982 F. Supp. 503, 513 (N.D. Ohio 1997) (distinguishing *Netcom* on the ground that the system operator had a policy of encouraging subscribers to upload files and its employees viewed and moved the uploaded files).

[15] 982 F. Supp. at 513.

[16] CoStar Grp., Inc. v. LoopNet, Inc., 373 F.3d 544, 550 (4th Cir. 2004) (real estate company employees checked user uploads for blatant infringement before posting them); *see also* Cartoon

In recent years, three district court decisions—two of them involving digital file lockers—have upheld (against 12(b)(6) challenge) direct infringement claims brought against online service providers, on the ground that certain organizational techniques and marketing initiatives meet the volitional conduct requirement.[17] In *Usenet*, for example, several record companies sued an online subscription bulletin board that was being used to share plaintiffs' copyrighted content. Following the reasoning in *Russ Hardenburgh*, the court held that by programming its system to dedicate servers to specific types of files, and by taking "active steps, including both automated filtering and human review, to remove access to certain categories of content, and to block certain users," defendant had directly infringed plaintiffs' copyrights as a matter of law.[18]

B. Secondary Liability

Commentators disagree as to whether the Copyright Act of 1976 explicitly recognizes indirect liability.[19] Nevertheless, as a matter of both statutory authority and common law, courts have long imposed liability on third parties to direct infringement pursuant to two distinct but often muddled doctrines: contributory infringement and vicarious liability.[20]

Network LP v. CSC Holdings, Inc., 536 F.3d 121, 131 (2d Cir. 2008). The court in *Cartoon Network* explained the volitional act requirement in the context of a television service provider's liability for its customers' allegedly infringing use of its digital video recording machines: "the person who actually presses the button to make the recording supplies the necessary element of volition, not the person who manufactures, maintains, or, if distinct from the operator, owns the machine." *Id.*

[17] Arista Records LLC v. Usenet.com, 633 F. Supp. 2d 124, 148–49 (S.D.N.Y. 2009); Capitol Records, Inc. v. MP3tunes, LLC, No. 07 Civ. 9931, 2009 U.S. Dist. LEXIS 96521 at *13 (S.D.N.Y. Oct. 16, 2009) (citing *Russ Hardenburgh* and *Usenet* in denying a motion to dismiss a direct infringement claim where defendant music locker collected and organized links for its customers to listen to and download); Perfect 10, Inc. v. Megaupload Ltd., No. 11 cv 0191, 2011 U.S. Dist. LEXIS 81931 at *13 (S.D. Cal. 2011). In *Megaupload*, the court denied a motion to dismiss a direct infringement claim, applying this reasoning to an online storage site widely used to share copyrighted films, where the site paid and encouraged users to upload popular files, paid third party sites to maintain inventory of available files, and created distinct websites dedicated to specific types of content. *Megaupload*, 2011 U.S. Dist. LEXIS 81931 at *12–*13.

[18] *Russ Hardenburgh*, 633 F. Supp. 2d at 148.

[19] *Compare* Douglas Lichtman & William Landes, *Indirect Liability for Copyright Infringement: An Economic Perspective*, 16 HARV. J. LAW & TECH. 395, 396 (2003) ("[T]he Copyright Act of 1976 does not explicitly recognize the possibility of indirect liability."), *with* 6 WILLIAM F. PATRY, PATRY ON COPYRIGHT § 21.43 (2011) (citing legislative history of the 1976 Act to the effect that section 106 includes the phrase "to authorize" for the specific, intended purpose of providing for indirect liability).

[20] Lichtman & Landes, *supra* note 19, at 396.

1. Contributory Infringement

Courts have established two elements necessary to a finding of contributory infringement: the accused party must have knowledge of the infringing activity, and she must "materially contribute" to the infringing conduct.[21]

a. Knowledge

While courts agree that the knowledge requirement should be objective, many have had difficulty in deciding the degree of knowledge necessary to justify imposition of liability, particularly in file-sharing and internet-based cases.[22] The critical question is whether a showing of constructive knowledge is sufficient. That is, whether a plaintiff must prove actual knowledge of the infringing activity, or whether some middle standard should apply.[23] Constructive knowledge, or knowledge imputed to a defendant based on the nature of her conduct, has been held sufficient in several cases.[24]

Conversely, many courts, particularly in a line of digital-context cases, have applied a tighter standard—requiring a showing of actual knowledge of specific infringing activity.[25] The issue is complicated by the presence or absence of "substantial non-infringing uses" for the relevant product.[26]

b. Material Contribution

A defendant materially contributes to copyright infringement when she actively causes the infringer to commit the infringement, or when she "provide[s] the means by which the infringement occurs."[27] This second form of material contribution has been interpreted loosely, and many courts have held it satisfied where the defendant provided the "site and facilities" of the infringement.[28] A recent major Ninth Circuit

---

[21] Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162 (2d. Cir. 1971) ("[O]ne who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another, may be held liable as a 'contributory' infringer.").

[22] Craig A. Grossman. *From Sony to Grokster, The Failure of the Copyright Doctrines of Contributory Infringement and Vicarious Liability to Resolve the War Between Content and Destructive Technologies*, 53 BUFF. L. REV. 141, 151–52 (2005).

[23] *Id.* at 152 n.12; *see also* 6 PATRY, *supra* note 19, § 21.47.

[24] Cable/Home Comm. Corp. v. Network Prods., Inc., 902 F. 2d 829, 845 (11th Cir. 1990); Sega Enters. Ltd. v. MAPHIA, 948 F. Supp. 923, 933 (N.D. Cal. 1996); *In re* Aimster Copyright Litig., 334 F.3d 643 (7th Cir. 2003).

[25] *See* Perfect 10, Inc. v. Amazon.com, Inc, 508 F.3d 1146, 1172 (9th Cir. 2011) (holding that "a computer system operator can be held contributorily liable if it "has *actual* knowledge that *specific* infringing material is available using its system") (emphasis in original) (quoting A&M Records v. Napster, Inc., 239 F.3d 1004, 1022 (9th Cir. 2001)); MGM Studios, Inc. v. Grokster, Ltd., 380 F.3d 1154, 1162 (9th Cir. 2004), *rev'd on other grounds*, 545 U.S. 913 (2005).

[26] Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 442 (1984).

[27] 6 PATRY, *supra* note 19, § 21.48.

[28] Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259 (9th Cir. 1996). Vendors at a swap meet sold thousands of infringing recordings. The owner of the copyrights in many of those works sued the swap meet, alleging *inter alia*, contributory and vicarious copyright infringement. *Id.* Since the

case suggests reining in this expansive interpretation to avoid the substantial costs of imposing liability on peripheral parties to Internet transactions.[29] In *Visa*, the court held that there was no material contribution where defendant processed online payments for websites that sold infringing photographs.[30] Further, it distinguished *Amazon.com* on the ground that payment systems' contribution was more attenuated than that of search engines: "there is an additional step in the causal chain: Google [a defendant in *Amazon.com*] may materially contribute to infringement by making it fast and easy for third parties to locate and distribute infringing material, whereas Defendants make it easier for infringement to be *profitable*, which tends to increase financial incentives to infringe, which in turn tends to increase infringement."[31] The majority's narrowed reading prompted a rigorous dissent.[32]

2. Vicarious Liability

While contributory infringement requires evidence of culpable action, vicarious liability, finding its origins in the strict liability principles of respondeat superior, focuses on the defendant's "right and ability to control" the infringing activity and whether the defendant stands to receive a financial benefit from it.[33] Importantly, vicarious liability is imposed where these two elements "coalesce,"—where the financial benefit is secured by the right to control, and thus where the policy goal of promoting self-regulation is likely to be effectuated.[34]

Defendant's knowledge of the infringing activities was not in dispute, the only issue was whether the defendant materially contributed to the infringing activity. *Id.* at 264. In holding the defendant liable for contributory infringement and eschewing the district court's "expressly promoted or encouraged" standard, the court argued that by providing the vendors (direct infringers) with a variety of services, including "space, utilities, parking, advertising, plumbing, and customers," the defendants had contributed sufficiently to warrant imposition of contributory liability. *Id.* This looser standard is commonly referred to as the "site and facilities rule." *See also Amazon*, 487 F.3d at 729 ("[Defendant] could be held contributorily liable if it had knowledge that infringing Perfect 10 images were available using its search engine, could take simple measures to prevent further damage to Perfect 10's copyrighted works, and failed to take such steps.").

[29] Perfect 10, Inc. v. Visa Int'l Serv. Ass'n, 494 F.3d 788, 797–98 (9th Cir. 2007).

[30] *Id.*

[31] *Id.* at 797.

[32] *Id.* at 811–14 (Kozinski, J., dissenting). Judge Kosinski argued that *Amazon* was not distinguishable and that the majority had turned its back on not only that case, but *Fonovisa*, *Napster*, and *Grokster* as well. *Id.* at 813. "The majority makes some very new—and very bad—law here." *Id.* at 814. *See also* 3 NIMMER, *supra* note 13, § 12.04[A][3][a] (finding the majority opinion "difficult to understand coherently," and endorsing Judge Kozinski's dissent: "In sum, although the Ninth Circuit has spoken to the issue of contributory copyright infringement far more often and more recently than any other tribunal, *Visa International* leaves its jurisprudence indeterminate.").

[33] Adobe Sys. Inc. v. Canus Prods., Inc., 173 F. Supp. 2d 1044, 1053 (C.D. Cal. 2001). *See also* Lichtman & Landes, *supra* note 19, at 398. The authors posit three policy rationales for vicarious liability in the context of copyright infringement: (1) providing incentives to self-police for infringement, (2) reducing costs by allowing copyright owners to pursue one lawsuit rather than go after the multitude of direct infringers, and (3) ensuring that adequate relief can be granted by removing the specter of bankrupt direct infringers). *Id.*

[34] Shapiro, Bernstein & Co. v. H. L. Green Co., 316 F.2d 304, 307–08 (2d Cir. 1963)

> When the right and ability to supervise coalesce with an obvious and direct financial interest in the exploitation of copyrighted materials-even in the absence

a. Right and Ability to Control

The "right and ability to control" element refers to the defendant's ultimate right to exclude infringers from using its service or revoke their capacity to infringe.[35] As vicarious liability has its roots in the so-called "dance hall cases,"[36] "right and ability to control" analysis focuses on the location (whether physical or digital) where the infringement took place, and asks whether the defendant could control what happened there.[37]

b. Financial Benefit

In the dance hall cases and their progeny, the financial benefit required for imposition of vicarious liability had to be "obvious and direct."[38] In the time since those cases were decided, courts have extended that limited understanding of the requirement.[39] Many courts now ask whether the presence of infringing activity drew potential customers to the place of business.[40] This expansive interpretation has also found particular application in the Internet context.[41]

> of actual knowledge that the copyright monopoly is being impaired . . . the purposes of copyright law may be best effectuated by the imposition of liability upon the beneficiary of that exploitation . . . our judgment will simply encourage [defendant] to ["police carefully the conduct of its (employee)"], thus placing responsibility where it can and should be effectively exercised.

Id. (internal citations omitted).

[35] *Id.* at 308; *see also Visa Int'l*, 494 F.3d 788 at 804 n.15. The court in *Visa* held an online payment processer not vicariously liable for infringement. *Visa*, 494 F.3d at 804 n.15. It distinguished *Napster*, which held a peer-to-peer system operator vicariously liable for its users' direct infringement, and followed the 9th Circuit decision in *Grokster*, which held a peer-to-peer system operator not vicariously liable for its users' infringement

> in part because they could not block individual users or remove copyrighted material from the network. Defendants have no ability to actually remove infringing material from the Internet or directly block its distribution. This distinguishes credit card companies from Napster, which could block access to the tools needed for the easy reproduction and distribution of the actual infringing content.

Id.

[36] *See, e.g.,* Herbert v. Shanley, 242 U.S. 591 (1917) (holding a hotel vicariously liable where its hired musicians publicly performed copyrighted music without authorization).

[37] Grossman, *supra* note 22, at 249–53. Professor Grossman argues that, due to the ever-expanding reach of digital networks [and the correspondingly ever-expanding control of system operators], application of this location-based reasoning in the digital realm implicates Fourth Amendment and right to privacy concerns.

[38] *Shapiro*, 316 F.2d at 307.

[39] Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 263 (9th Cir. 1996). The court in *Fonovisa* rejected Defendant's argument that the financial benefit must be "a commission, directly tied to the sale of particular infringing items," and contended instead that the essence of the financial benefit requirement in the dance hall cases was that the "infringing performances enhance[d] the attractiveness of the venue to potential customers." *Id.* If the infringing activity is a "draw" for customers, the financial benefit requirement is met. *Id.*

[40] *See* Polygram Int'l Publ'g, Inc. v. Nevada/TIG, Inc., 855 F. Supp. 1314, 1326 (D. Mass. 1994) (citing Judiciary Committee report on the 1976 Copyright Act for the proposition that in order to

3. Sony and "substantial non-infringing uses"

In *Sony Corp. of America v. Universal City Studios, Inc.*, the Supreme Court was tasked with deciding whether to impose secondary liability on Sony for manufacturing and distributing Betamax machines that were capable of reproducing copyrighted works.[42] The Court adopted the "staple article of commerce" doctrine from patent law, holding that "the sale of copying equipment ... does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes. Indeed, it need *merely* be *capable of substantial non-infringing uses*."[43] This expansive language would seem to provide a powerful defense to indirect liability, but in practice very few courts have ruled in favor of such a defense since *Sony*.[44]

4. Grokster and inducement liability

21 years after *Sony*, in *MGM Studios, Inc. v. Grokster, Ltd.*,[45] the Supreme Court once again had occasion to address the issue of a technology company's liability for the infringing activities of its customers. The Court declined to elaborate on the Sony rule, instead adopting another factually appropriate doctrine from patent law-inducement of infringement.[46] Under this new understanding of secondary liability for copyright infringement, "one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties."[47] Commentators and courts disagree as to whether the *Grokster* decision

---

meet the financial benefit requirement a defendant need only "expect commercial gain from the operation and either direct or indirect benefit for the infringing performance").

[41] Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1171 (C.D. Cal. 2002) (following the "draw" logic from *Fonovisa*: "Cybernet benefits directly from these infringing sites to the extent that they have brought in new users because the new customers pay Cybernet directly"); *see also* A&M Records v. Napster, Inc., 239 F.3d 1004, 1023 (9th Cir. 2000) ("Napster's *future revenue* is directly dependent upon 'increases in user base.'") (emphasis added).

[42] Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417 (1984).

[43] *Id.* at 442 (emphasis added). Since the court held time-shifting of television programs constituted fair use, Sony was not contributorily liable for selling Betamax machines to the public. *Id.; see also* 35 U.S.C. § 271(c) (2012) (providing that the sale of a "staple article or commodity of commerce suitable for substantial non-infringing use" does not constitute patent infringement).

[44] *See* Jessica Litman, *The Sony Paradox*, 55 CASE W. RES. L. REV. 917, 951–952 (2005) (collecting cases in which courts declined to accept the Sony defense); *see also In re* Aimster Copyright Litig., 334 F. 3d 643, 651 (7th Cir. 2003) (holding mere capability of substantial non-infringing use insufficient to assert a Sony defense and requiring evidence of actual non-infringing use).

[45] Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005).

[46] *See* 35 U.S.C. § 271(b) ("Whoever actively induces infringement of a patent shall be liable as an infringer.").

[47] *Grokster*, 545 U.S. at 936–37. The Court distinguished *Sony*: *"Sony* barred secondary liability based on presuming or imputing intent to cause infringement solely from the design or distribution of a product capable of substantial lawful use, which the distributor knows is in fact used for infringement." *Id.* at 934. By contrast, the *Grokster* defendants' intent to cause infringement (to the level of active inducement) was established by extrinsic evidence: (1) They marketed themselves as an alternative to Napster, an infringing service, (2) they took no steps (such

created a new cause of action or merely put a gloss on existing copyright jurisprudence.[48]

C. Safe Harbors under the Digital Millennium Copyright Act

In 1998, Congress passed the Online Copyright Infringement Liability Limitation Act (OCILLA) as part of the DMCA, in an attempt to foster cooperation between content providers and online service providers and thereby minimize infringement.[49]

OCILLA establishes four distinct "safe harbors" [50]—each representing a carefully defined set of circumstances under which an online service provider is exempted from copyright liability.[51] To qualify for any of the four safe harbor exemptions, an online service provider must demonstrate compliance with subsection (i), which requires system operators to "adopt and reasonably implement" repeat infringer policies[52] and to accommodate certain "standard technical measures," to be defined by a broad consensus of interested parties.[53] Since no consensus has been reached with regard

---

as content filtering) to diminish infringement, and (3) their business plans isolated advertisement as the revenue stream and therefore depended on high-volume use of their service, and "the evidence shows that substantive volume is a function of free access to copyrighted work." *Id.* at 939–40. Thus, where the evidence shows that the defendant actively induced infringement, she does not get the benefit of the *Sony* defense. *Id.*

[48] *See* 3 NIMMER, *supra* note 13, § 12.04[A][4][b]. Nimmer argues that *Grokster* should be read as carving out a new theory of liability, but notes that it could be read as an elaboration of contributory liability. *Id.* He highlights the Ninth Circuit's divergent treatment of the *Grokster* precedent in *Amazon.com* and *Visa*. *Id.*

[49] 17 U.S.C. § 512 (2012); *see also* ALS Scan, Inc. v. RemarQ Cmtys., Inc., 239 F.3d 619, 625 (4th Cir. 2001) (quoting H.R. REP. NO. 105-796, at 72 (1998) (Conf. Rep.)).

> The DMCA was enacted both to preserve copyright enforcement on the Internet and to provide immunity to service providers from copyright infringement liability for "passive," "automatic" actions in which a service provider's system engages through a technological process initiated by another without the knowledge of the
> service provider.

Id.

[50] 17 U.S.C. § 512. The four safe harbors are: (a) Transitory digital network communications, (b) System caching, (c) Information residing on systems or networks at direction of users, and (d) Information location tools. *Id.*

[51] *See CoStar*, 373 F.3d 544 at 555.

> It is clear that Congress intended the DMCA's safe harbor for ISPs to be a floor, not a ceiling, of protection. Congress said nothing about whether passive ISPs should ever be held strictly liable as direct infringers or whether plaintiffs suing ISPs should instead proceed under contributory theories. The DMCA has merely added a *second step* to assessing infringement liability for Internet service providers, *after* it is determined whether they are infringers in the first place under the preexisting Copyright Act.

Id. (emphasis added).

[52] 17 U.S.C. § 512(i)(1)(A) ("a policy that provides for the termination in appropriate circumstances *of* subscribers and account holders of the service provider's system or network who are repeat infringers").

[53] *Id.* § 512(i)(1)(B). The statute defines "standard technical measures" as

> technical measures that are used by copyright owners to identify or protect copyrighted works and--

to standard technical measures, this second requirement has essentially been nullified by practice in the years since passage of the DMCA.[54]

In the context of cloud storage, the most relevant safe harbor is § 512(c).[55] The statute conditions the exemption on the presence of one of three conditions. The first of these, the knowledge requirement, is itself a three-pronged, disjunctive condition—that the online service provider:

> **(A)(i)** does not have actual knowledge that the material or an activity using the material on the system or network is infringing;
> **(ii)** in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; ***or***
> **(iii)** upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material[.][56]

Given that one of these is met, the service provider must also show that it

> **(B)** does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; ***and***
> **(C)** upon notification of claimed infringement . . . responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.[57]

Importantly, recent case law expresses uncertainty as to whether the § 512(c) safe harbor protects webhosts from claims of vicarious liability,[58] and whether webhosts that induce infringement under the Grokster standard are ineligible for the safe harbor exemption.[59]

D. The Controversial Elements of Cyberlockers

Cyberlockers execute a variety of business plans, incorporating various components in different ways. Importantly, many, even most cyberlockers have

---

> (A) have been developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process;
> (B) are available to any person on reasonable and nondiscriminatory terms; and
> (C) do not impose substantial costs on service providers or substantial burdens on their systems or networks.

Id. § 512(i)(2).

[54] *See* 3 NIMMER, *supra* note 13, § 12B.02[B][3][a] ("Even as of many years after enactment of the [OCILLA], it is unclear whether there is any such thing as "standard technical measures.").

[55] 17 U.S.C. § 512(c). The service provider must also follow a specified procedure to designate an agent to receive notices of infringement from copyright owners, and the notices must meet a series of technical and substantive requirements. *Id.* § 512(c)(3).

[56] *Id.* § 512(c)(1)(A) (emphasis added).

[57] *Id.* § 512(c)(1)(B)–(C) (emphasis added).

[58] *See* Edward Lee, *Decoding the DMCA Safe Harbors*, 32 COLUM. J. L. & ARTS 233, 235–46 (2009) (discussing competing theories and recent case law as to whether § 512(c) exempts webhosts from vicarious liability).

[59] *Compare* Viacom Int'l Inc. v. YouTube, Inc., 718 F. Supp. 2d 514, 526 (S.D.N.Y. 2010) (holding that *Grokster*'s "application to the particular subset of service providers protected by the DMCA is strained"), *with* Viacom Int'l, Inc., v. YouTube, Inc., 676 F. 3d 19, 40 (2d Cir. 2012) (positing in dictum that "inducement of copyright infringement under [*Grokster*] . . . might . . . rise to the level of control under § 512(c)(1)(B).").

avoided the dark cloud of massive infringement allegations and are perceived as legitimate.[60] It is instructive, then, to highlight the features that copyright owners (and governments) typically find objectionable: (1) public (as opposed to password-protected) sharing capability;[61] (2) direct linking;[62] (3) lack of search function;[63] and(4) rewards programs.[64]

Password-protected private storage is the core service of many cyberlockers, and is clearly non-infringing.[65] But even those cyberlockers typically seen as legitimate offer public sharing, and with good reason—a user should be entitled, for example, to tweet a publicly accessible link to her copyrighted short story. The problem, at least as copyright owners see it, is that the same feature that allows her to share her story, when combined with other features of the cyberlocker business plan, facilitates large-scale copyright infringement.

Many cyberlockers allow users with no connection to a file's uploader to download that file.[66] Though many of them disaggregate search functionality, copyright owners argue that this tactic has little practical effect on the user who is looking to find a specific file.[67] That is, instead of using a search tool on the website itself, a user can just search on a regular search engine for the name of a work along with the name of a cyberlocker (e.g. "hunger games mediafire") and out will pop a series of links, both to download pages themselves and to third-party sites that aggregate download links to files hosted by cyberlockers.[68] This is a classic "damned if you do, damned if you don't" situation. Internal search functionality has been looked to as evidence of intent to foster infringement in the past because it makes it easier for a user to find

---

[60] *See, e.g.,* Jared Newman, *How to Choose Between Cloud Storage Services Like Google Drive and Dropbox*, TIME MAG. (Apr. 27, 2012), http://www.techland.time.com/2012/04/27/how-to-choose-between-cloud-storage-services-like-google-drive-and-dropbox/ (analyzing strengths and weaknesses of four popular legitimate file locker services).

[61] *See* Complaint at 5, Liberty Media Holdings, LLC v. FF Magnat Ltd., No. 12-cv-01057 (D. Nev. June 20, 2012), *available at* www.xbiz.com/docs/xbiz/news/150218_corbin fisher v oron 062012.pdf ("the primary purpose of this storage capacity and allowing rapid public access to it is the unauthorized use and exchange of copyrighted works.").

[62] *See* Plaintiffs' Motion and Memorandum of Law in Support of Summary Judgment at 7, Disney Enters. v. Hotfile, Inc., No. 11-20427 (S.D. Fl. Mar. 5, 2012) [hereinafter Hotfile Plaintiffs' Motion for Summary Judgment] (describing the importance of direct linking to Hotfile's Affiliate Program, which allegedly induced infringement).

[63] *Id.* at 4 n.1, (arguing that the fact that the lack of a "technological or business reason why Hotfile does not have a search function on its own website . . . reflects Hotfile's attempt to conceal, or blind itself to, the rampant copyright infringement it fosters.").

[64] *See* Complaint at 5, Flava Works, Inc. v. Does 1-26, No. 12-cv-05844 (N.D. Ill. July 24, 2012), 2012 WL 3096376 (alleging that rewards program satisfied direct financial benefit element of contributory and inducement causes of action).

[65] *See* Roger Parloff, *Megaupload and the Twilight of Copyright*, FORTUNE, July 23, 2012, at 131 (identifying password-protection as a feature that renders a system "poorly suited for mass distribution of copyrighted materials.").

[66] Richard Raysman & Peter Brown, *Cyberlockers, File-Sharing, and Infringement in the Cloud*, LAW.COM (Sept. 12, 2012), http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1347193574468&thepage=1 (explaining that "rogue" cyberlockers function by providing a publicly accessible link which can be accessed by way of third-party aggregators).

[67] Hotfile Plaintiffs' Motion for Summary Judgment, *supra* note 62, at 4.

[68] *Id.*; *"Hunger Games Mediafire" Search Results*, GOOGLE.COM, http://www.google.com (search "hunger games mediafire") (last visited Nov. 8, 2012).

infringing works on the system,[69] but removing search functionality indicates an effort to knowingly shield oneself from liability.[70]

Some cyberlockers also simply pay uploading users—based on the size of uploaded files and the number of times those files are downloaded ("pay per download" or "PPD") or the number of premium memberships sold from the user's download pages ("pay per sale" or "PPS").[71]

E. Hotfile and Megaupload

In light of the growing popularity of cyberlockers, many have drawn the ire of copyright holders in recent years. Most recently, and most notably, the cyberlockers Megaupload and Hotfile have met with litigation.

After its launch in 2005, Megaupload rose to a position of leadership in the growing cyberlocker industry.[72] On megaupload.com as well as various subsidiary sites, the company offered a free storage service supported by advertising revenue as well as a premium membership service for which they charged one-time fees based on length of service.[73]

In January 2011, Perfect 10, a notoriously litigious adult entertainment company, brought suit against Megaupload, alleging *inter alia* direct, contributory, and vicarious copyright infringement.[74] The parties to the lawsuit settled their dispute early in the discovery process and the case was dismissed.[75] This paper's

---

[69] *See, e.g.,* A&M Records, Inc. v. Napster, Inc., 239 F. 3d 1004, 1023 (9th Cir. 2001) (citing the fact that Napster could have located infringing material listed on its search indices in holding Napster liable for vicarious infringement).

[70] Hotfile Plaintiffs' Motion for Summary Judgment, *supra* note 62, at 4 n.1.

[71] *See, e.g. Earn*, RAPIDGATOR, http://www.rapidgator.net/article/resource (follow "Pay per download" and "Pay per sale" hyperlinks) (last visited Nov. 8, 2012) (detailing payout rates for its PPD and PPS systems).

[72] According to the web analytics firm Alexa Internet, Megaupload was the 73rd most popular website in the world between 7/20/2010 and 10/20/2010. *Megaupload.com Site Info*, ALEXA.COM, http://www.web.archive.org/web/web.php (accessed by searching for "megaupload" in the Internet Archive index). Based on July 2011 data collected by Google, Megaupload was the second most visited file sharing website in the world and the 91st most popular web site in the world. *The 1000 Most-Visited Sites on the Web*, GOOGLE.COM, http://www.google.com/adplanner/static/top1000 (last visited Nov. 8, 2012). Its subsidiary, megavideo.com, was ranked 129th in overall popularity. *Id.*

[73] Indictment at 4, United States v. Dotcom, No. 1:12CR3 (E.D. Va. Jan. 5, 2012). Free members were limited to 200 GB of storage at a maximum of 2 GB per file, and the frequency and speed of their downloads was restricted. *Difference Between Megaupload and Rapidshare*, DIFFERENCEBETWEEN.NET, http://www.differencebetween.net/technology/internet/difference-between-megaupload-and-rapidshare/ (last visited Dec. 29, 2012). Premium users had access to unlimited storage capacity, could download multiple files at the same time, and are subject to substantially less advertising. *Premium*, MEGAUPLOAD, http://www.megaupload.com/?c=premium (last visited Oct. 18, 2011) (currently unavailable due to domain seizure – screen-capture on file with the John Marshall Review of Intellectual Property Law). The fees for premium service were determined by the user's selection of one of seven service plans- €3.99 for one day, €9.99 for one month, and so on, up to €199.99 for a "lifetime platinum" membership. *Id.*

[74] Complaint at 9–10, Perfect 10, Inc. v. Megaupload, Ltd., No. 11-cv-0191 (S.D. Cal. July 26, 2011), 2011 U.S. Dist. LEXIS 81931 [hereinafter Megaupload Complaint].

[75] Order Granting Joint Motion to Dismiss with Prejudice, *Megaupload*, No. 11-cv-0191 (Oct. 18, 2011).

discussion of that case will focus on the district court's July 2011 ruling on Megaupload's motion to dismiss.[76] In January 2012, working in conjunction with law enforcement authorities in eight countries, the Department of Justice shut down the Megaupload sites and brought unprecedented criminal charges against Megaupload, its subsidiaries, and seven key individuals involved in its operations.[77] The breathtaking indictment[78] alleges criminal secondary infringement, a theory that has not yet been tested in court.[79]

Hotfile is another popular cyberlocker in the mold of Megaupload.[80] For its part, it has been sued multiple times by copyright holders.[81] In February 2011, a collection of major motion picture studios sued Hotfile, alleging direct and secondary infringement of their copyrights. [82]

When a user uploads a file to the site, the user receives a unique download link.[83] The file can then be downloaded by anyone in possession of that download link.[84] Like Megaupload, Hotfile imposes use limits on unregistered and "free" users and removes these limits for its premium users, who pay fees.[85] The site includes an intellectual property policy that complies fully with the DMCA.[86] The complaint

---

[76] *Megaupload*, No. 11-cv-0191.

[77] Press Release, Dep't of Justice, Justice Dep't Charges Leaders of Megaupload with Widespread Online Copyright Infringement (Jan. 19, 2012), *available at* http://www.justice.gov/opa/pr/2012/January/12-crm-074.html.

[78] Indictment, United States v. Dotcom, No. 1:12CR3 (E.D. Va. Jan. 5, 2012).

[79] *See* Nate Anderson, *Government Admits Defeat, Gives Back Seized Rojadirecta Domains*, ARS TECHNICA (Aug. 29, 2012, 3:23 PM), http://arstechnica.com/tech-policy/2012/08/government-goes-0-2-admits-defeat-in-rojadirecta-domain-forfeit-case/. The Department of Justice recently dismissed its own case alleging criminal secondary infringement against Puerto 80 Projects, owner of a Spanish website that allowed users to post recordings and streams of sporting events. *Id.*

[80] As of November 8, 2012, Alexa Internet ranked Hotfile 659th in global popularity using data from the interval between August 8, 2012 and November 8, 2012. *Hotfile.com: Site Info*, ALEXA.COM, http://www.alexa.com/siteinfo/hotfile.com (last visited Nov. 8, 2012). Hotfile's ranking and overall performance across various metrics has declined steadily and significantly in the wake of its involvement in litigation. *Id.* Hotfile's traffic rank, for example, has dropped from comfortably within the top 200 most visited websites to its current position outside the top 600. *Id.* Graphs indicating declines across seven different metrics can be accessed by clicking the "Traffic Stats" tab, selecting the appropriate tab for each metric, and setting the time period to "Max."

[81] Liberty Media Holdings, LLC v. Hotfile.com, No. 09-02396 (N.D. Tex. Dec. 16, 2009); Perfect 10, Inc. v. Hotfile Corp., No. 10-02031 (S.D. Cal. Sept. 29, 2010); Liberty Media Holdings, LLC v. Hotfile Corp., No. 11-20056 (S.D. Fla. Jan. 6, 2011);

[82] Complaint at 8–11, Disney Enters., Inc. v. Hotfile Corp., No. 11-20427 (S.D. Fla. Feb. 8, 2011) [hereinafter Hotfile Complaint].

[83] *Terms of Service*, HOTFILE, http://hotfile.com/terms-of-service.html (last visited Nov. 8, 2012).

[84] *Id.*

[85] *Premium Member Program*, HOTFILE, http://hotfile.com/premium.html (ast visited Nov. 8, 2012). Hotfile's premium fees are also dependent on the user's selection from three available service plans- $9 for one month, $35 for six months, and $55 for one year. *Id.* All premium members receive unlimited download access, and as the plans get more expensive a user is given a larger traffic allowance for her hotlinks (she can allow non-users to download her files at premium speeds). *Id.*

[86] *Intellectual Property Policy*, HOTFILE, http://hotfile.com/ippolicy.html (last visited Oct. 19, 2011). The policy also offers Special Rightsholder Accounts to copyright owners who "have given or may be required to give repeated notifications" of infringing material. *Id.* These accounts allow the owner to, in good faith, submit URLs for automatic takedown without having to complete a sufficient notice for each instance of infringement. *Id.*

focuses on four significant elements of Hotfile's service: (1) the site gradually increases payments to uploading users based on file size and number of downloads;[87] (2) the site increases payments based on how broadly users disseminate their download links;[88] (3) the site pays third-party sites when a user follows a link from the third-party site to a Hotfile-hosted download page, and, once there, signs up to be a Hotfile premium member;[89] and (4) the site includes statements which make plain Hotfile's intent to incentivize copyright infringement and dis-incentivize non-infringing use of its service.[90]

---

[87] Complaint at 9–10, *Hotfile*, No. 11-20427. At the time of filing and for a substantial period thereafter, the company paid uploading users each time one of their files was downloaded 1000 times by other users. *Id.*; *see also* First Amended Answer at 5–6, *Hotfile*, No. 11-20427 [hereinafter Hotfile Amended Answer] (admitting these allegations in pertinent part). The rate paid for each 1000 downloads was increased with the size of the file and the "rank" of the user. *Id.* The user's rank was determined by two factors: "1. The ratio of the users that downloaded your files and the users that become premium based on your uploaded files;" and "2. The ratio of uploaded files to number of downloads." *Id.* at 6.

The MPAA points out that based on this scheme, "a single uploaded file that is downloaded 50,000 times is more highly rewarded than 50 uploaded files downloaded 1,000 times each." Complaint at 9–10, *Hotfile*, No. 11-20427. It argues that by implementing this business plan, Hotfile "incentivizes users to upload only highly popular works so as not to 'waste' Hotfile's server storage space with files that are not popular and not being downloaded by massive numbers of users." *Id.*

Interestingly, Hotfile has since changed its affiliate program to a pay per sale (PPS) system—whereby users are paid according to how many downloaders purchase premium subscriptions. *Affiliate Program*, HOTFILE, http://hotfile.com/affiliate.html (last visited Nov. 21, 2012).

[88] *Id.* As the MPAA and studios argue, this scheme also disincentivizes non-infringing use of the service. Because the ratio system is fluid, it penalizes users for uploading less popular files. *Id.* at 10–11. Furthermore, Hotfile deletes files (of non-premium users) that have not been downloaded in 90 days. *Frequently Asked Questions*, HOTFILE, http://hotfile.com/faq.html (last visited Nov. 21, 2012).

[89] *Affiliate Program*, HOTFILE, http://web.archive.org/web/20110623181809/http://hotfile.com/affiliate.html (accessed by searching "http://hotfile.com/affiliate.html" in the Internet Archive Index).

> For site owners: Get 5% commission of all premium accounts sold through your site. For every referrer that comes from your site and buys premium, you will get 5% of the account's price. No matter if download link is yours or you've found it elsewhere! Post interesting download links in your site, blog or forum and earn big money.

Id.; see also Hotfile Amended Answer, *supra* note 87, at 7. This language has since been deleted, and Hotfile has changed its referral program, so that it only applies to individual users and not third-party sites. *Affiliate Program*, *supra* note 89.

[90] Hotfile Amended Answer, *supra* note 87, at 2.

> Hotfile admits that at one time, the FAQ page of the hotfile.com website contained the phrase '*[u]pload files only if you intend to promote them*' and the Affiliate page of the hotfile.com website contained the phrase '*to encourage the good promoters by increasing their earnings and* ***to reduce the earnings for uploaders that mainly use the free Hotfile resources for storage***.'

Id. (emphasis added).

II. ANALYSIS

In the wake of the Megaupload indictment, many important cyberlockers have significantly altered or even shut down their services.[91] Paradoxically, though, due to a number of procedural issues beyond the scope of this Comment, as well as the elevated burden that attends a criminal copyright infringement case, there is ample room for skepticism that the case against Megaupload will be heard on the merits.[92] Thus, the *Hotfile* case stands, at least in the view of some commentators, as an especially significant test case for the legality of cyberlockers.[93] Accordingly, this section will use the facts, judicial opinions, and legal argument from these two cases to analyze the status of cyberlockers under the currently applicable legal framework introduced above.

A. Direct Infringement

In *Perfect 10 v. Megaupload*, the Southern District Court of California focused its direct infringement analysis on three elements of Megaupload's business plan that were targeted in the complaint. First, the court inferred that the company's use of multiple websites represented an effort to "streamline users' access to different types of media."[94] Second, the court looked to Megaupload's Rewards plan which, at least according to the complaint, incentivized users to upload popular files (which are more likely to infringe).[95] Third, the court pointed to the allegation that Megaupload paid affiliated websites who indexed its available files to make them available for search.[96] Finally, following *Usenet*,[97] the court gave credence to Perfect 10's allegation that "at a minimum, [Megaupload] is *plausibly aware* of the ongoing,

---

[91] *See, e.g.,* enigmax, *FileServe and Wupload Exit the File-Sharing Business*, TORRENTFREAK (Apr. 3, 2012), http://www.torrentfreak.com/fileserve-and-wupload-exit-the-file-sharing-business-120403/. In addition to the Megaupload indictment, an Australian pornographer operating the website "stopfilelockers.com" has undertaken a fairly successful effort to convince payment systems to cut off services to many cyberlockers. STOPFILELOCKERS, http://www.stopfilelockers.com (last visited Dec. 2, 2012); enigmax, *90 Days of Killing Cyberlockers: 50 Dead, More Than 500 Injured*, TORRENTFREAK (Oct. 6, 2012), http://www.torrentfreak.com/90-days-of-killing-cyberlockers-50-dead-more-than-500-injured-121006/.

[92] *See generally* Eriq Gardner, *Megaupload Judge Says He Doesn't Know if There Will Ever be a Trial*, HOLLYWOOD REP. (Apr. 20, 2012, 6:38 PM), http://www.hollywoodreporter.com/thr-esq/megaupload-trial-kim-dotcom-314657 (surveying the myriad complicating issues involved in the case).

[93] *See* Terrence Hart, *Copyright Liability for Filelockers: Disney v. Hotfile*, COPYHYPE (Aug. 20, 2012), http://www.copyhype.com/2012/08/copyright-liability-for-filelockers-disney-v-hotfile/ (noting that the case "may prove influential in shaping copyright law online").

[94] Perfect 10, Inc. v. Megaupload, Ltd., No. 11-cv-0191 (S.D. Cal. July 26, 2011), 2011 U.S. Dist. LEXIS 81931 .

[95] *Id.* at 7*; see also* Complaint, *Megaupload*, No. 11-cv-0191, at 6–7.

[96] Complaint, *supra* note 95, at 7.

[97] Arista Records LLC v. Usenet.com, 633 F. Supp. 2d 124, 147 (S.D.N.Y. 2010). Recall that the court in *Usenet* denied the defendant's motion to dismiss the direct infringement claim because the defendant's online message board dedicated servers specifically to facilitate upload/download of mp3 files, was aware that its service was being used to exchange infringing files. *Id.*

rampant infringement taking place on its websites."[98] Though the court's analysis appears to establish the elements of contributory rather than direct infringement, it found this reasoning sufficient to justify denial of Megaupload's motion to dismiss.[99]

Conversely, in *Hotfile*, the court adhered to a conventional interpretation of the *Netcom* standard, attacking the *Usenet* reasoning which would later be adopted by the *Megaupload* court.[100] The court argued that such reasoning "ignores the language of *Netcom* and other cases following *Netcom*. As the Fourth Circuit put it, 'knowledge coupled with inducement,' or 'supervision coupled with a financial interest in the illegal copying' gives rise to secondary liability, not direct-infringement liability."[101]

The *Netcom* rule is malleable, and cyberlocker cases give judges excellent opportunities to manipulate it. Just as the material contribution test in contributory infringement has been relaxed by the courts,[102] so too the volitional requirement may be expanded to impose liability according to the conviction of the court. Now that the broad interpretation that *Usenet* extrapolated from *Russ Hardenburgh* seems to be gaining some traction, some uncertainty has been introduced.[103] It is important to note, however, that the recent trend consists entirely of district court decisions, and that the practical efficacy of the *Netcom* approach counsels in favor of retaining that rule in spite of the theoretical weaknesses this new wave of opinions has exploited.

B. Contributory Infringement

In the *Megaupload* case, the Defendant argued that the Plaintiffs had failed to adequately allege (1) the underlying direct infringement, (2) that Megaupload had specific knowledge of the underlying infringement (if any did in fact occur), and (3) that Megaupload had the right and ability to control any infringing conduct.[104] The defendant did not dispute the allegation that (assuming infringement occurred) it materially contributed to its users' direct infringement.[105]

---

[98] *Megaupload*, No. 11-cv-0191, at 7.

[99] *Id*.

[100] *Hotfile,* No. 11-20427, at 6.

[101] *Id. (*quoting CoStar Grp., Inc. v. LoopNet, Inc., 373 F.3d 544, 550 (4th Cir. 2004)).

[102] *See supra* note 28 and accompanying text.

[103] Eric Goldman, *Catching up on Four Months of Copyright Cases: Myxer, Hotfile, Megaupload, Flava Works, Zediva, Blue Nile, Perfect 10, Rojadirecta*. ERIC GOLDMAN TECH. & MARKETING L. BLOG (Aug. 12, 2011), http://blog.ericgoldman.org/archives/2011/08/catching_up_on.htm ("The fact is that all but the most passive of hosts or conduits take some affirmative steps towards customizing the downloader's experience, and trying to parse which of those steps constitute "volitional" conduct and which don't is leading to the inevitable doctrinal incoherence.").

[104] Memorandum of Points and Authorities in Support of Defendant Megaupload LLC's Motion to Dismiss at 4–6, Perfect 10, Inc. v. Megaupload, LLC, No. 11-cv-0191 (S.D. Cal. July 26, 2011) 2011 U.S. Dist. LEXIS 81931. Megaupload argued for application of a strict, "actual knowledge of specific instances of infringement standard." *Id.* at 5 (citing Perfect 10, Inc. v. Amazon.com, Inc, 508 F.3d 1146, 1172 (9th Cir. 2011).

[105] *Megaupload*, No. 11-cv-0191 at 9.

The court declined to impose a strict specific knowledge standard at the motion to dismiss stage.[106] Noting that a takedown notice, standing alone, may not represent sufficient evidence of knowledge, the court pointed to the various features of Megaupload's business plan[107] that supported a "plausible inference of knowledge,"[108] to the extent that "if Megaupload lacks knowledge of infringing activity, Plaintiff's allegations suggest such lack of knowledge is willful."[109]

In possession of a much clearer record, the *Hotfile* court held that the Studios' allegations regarding the nature of Hotfile's business plan were sufficient to survive a motion to dismiss.[110]

The *Hotfile* Plaintiffs contend in their Motion for Summary Judgment that, since for DMCA purposes Defendants had actual knowledge, red flag knowledge, or willful blindness with respect to the infringement occurring on their service, *a fortiori* they had knowledge sufficient to justify a finding of contributory infringement.[111] This conclusion is founded on the proposition, supported by a citation to five cases, that a plaintiff need not demonstrate that a contributory infringer had actual knowledge, but merely that the defendant "'had reason to know' of the infringing activity."[112]

For their part, the Defendants argue initially that they are entitled to the *Sony* exemption from liability, as their service is capable of substantial non-infringing uses.[113] On the strength of its current and potential non-infringing uses, Defendants maintain, Hotfile should be absolved from liability.[114] In the event that they are not entitled to *Sony* protection, Defendants claim that they are not contributory infringers because there is no evidence that Hotfile had actual knowledge of any specific files, and directly rebut Plaintiffs' assertion that actual knowledge is not required with their own five-case string citation.[115]

The proper interpretation of the *Napster* case is at the center of the parties' dispute. Defendants contend that *Napster* "is the seminal cases (sic.) *establishing* the 'actual knowledge' standard.'"[116] But Plaintiffs cite to *Napster* for the proposition that a contributory infringer need only "know or have reason to know" of the

---

[106] The court quotes the same standard from *Amazon* relied on by Megaupload in its Motion, but arguably proceeds to adopt a looser, constructive knowledge standard. *Id.* at 8. Such an approach is likely appropriate at the motion to dismiss stage and in light of the particular facts of this case.

[107] *See supra* notes 94–107 and accompanying text.

[108] *Megaupload*, No. 11-cv-0191, at 9.

[109] *Id.; see also In re* Aimster Copyright Litig., 334 F.3d 643, 650 (7th Cir. 2003) ("Willful blindness is knowledge").

[110] Disney Enters. v. Hotfile, 798 F. Supp. 2d 1303, 1310–11 (S.D. Fl. 2011). As in *Megaupload*, the court was willing to accept evidence of constructive knowledge at the motion to dismiss stage. *Id.*

[111] Hotfile Plaintiffs' Motion for Summary Judgment, *supra* note 62, at 33.

[112] *Id.* (quoting Cable/Home Comm. Corp. v. Network Prods., Inc., 902 F.2d 829, 846 (11th Cir. 1990)).

[113] Memorandum of Law of Defendants in Opposition to Plaintiffs' Motion for Summary Judgment at 28–30, *Hotfile*, No. 11-20427 (S.D. Fl. Mar. 5, 2012) [hereinafter Hotfile Defendants' Opposition Memorandum]. Defendants point out that their service can be and is used for distribution open-source software, for personal storage, for sharing Creative Commons-licensed films, and for distribution of public domain material. *Id.* at 28–29.

[114] *Id.* at 29.

[115] *Id.* at 31.

[116] *Id.*

infringing activity.[117] So which is it? The situation is confused by the fact that the court in *Napster* found that there was a factual basis for actual knowledge of specific infringement,[118] but a close reading of *Napster* nevertheless supports the Plaintiffs' case more strongly.

There, the court opened its contributory infringement analysis with the statement of law quoted in Plaintiffs' Motion.[119] It expressed its holding on the issue as follows: "the evidentiary record here supported the district court's finding that plaintiffs would likely prevail in establishing that Napster ***knew or had reason to know*** of its users' infringement . . . ."[120] Importantly, the court distinguished between the structure of Napster's system and the nature of Napster's conduct.[121] Hotfile emphasizes the court's assertion that "absent any specific information which identifies infringing activity, a computer system operator cannot be liable for contributory infringement merely because the structure of the system allows for the exchange of copyrighted material."[122] But this statement, read in context, necessarily leaves room for constructive knowledge to satisfy the knowledge requirement. That is, the court did not state a binary—that a system operator is liable when it has actual knowledge, and not liable when it does not have actual knowledge. Rather, the court declared that, absent any specific information identifying infringement, the operator may not be held liable *on account of the* ***structure*** *of her system*.[123] That language leaves open a third scenario—where the host lacks specific identifying knowledge, but has *operated* its system in such a way as to justify a finding that it *should have known* of the infringing activity. This reading is consistent with the initial statements of the knowledge requirement in both the *Napster* and *Netcom* cases; statements which were not abandoned by either court.[124]

C. Vicarious Liability

In *Megaupload*, the court followed the *Visa* court's formulation of "right and ability to control."[125] Since anyone with the appropriate URL could download an infringing file from its site, the court reasoned, Megaupload did not have the right

---

[117] Hotfile Plaintiffs' Motion for Summary Judgment, *supra* note 62, at 33.

[118] A&M Records v. Napster, Inc., 239 F.3d 1004, 1022 (9th Cir. 2001).

[119] *Id.* at 1020.

[120] *Id.* at 1021

[121] *Id.* at 1020 ("We are compelled to make a clear distinction between the architecture of the Napster system and Napster's conduct in relation to the operational capacity of the system.").

[122] *Id.* at 1021; Hotfile Defendants' Opposition Memorandum, *supra* note 113, at 31–32.

[123] *Napster*, 239 F.3d at 1021.

[124] *Id.* at 1020; Religious Tech. Ctr. v. Netcom, Inc., 907 F. Supp. 1361, 1373–74 (N.D. Cal. 1995) (framing issue as whether Defendant knew or should have known of the infringement).

[125] Perfect 10, Inc. v. Megaupload, Ltd., No. 11-cv-0191, 2011 U.S. Dist. LEXIS 81931, at *18 (S.D. Cal. July 26, 2011) (quoting Perfect 10, Inc. v. Visa Int'l Serv., Ass'n, 494 F.3d 788, 805 (9th Cir. 2007)) ("For vicarious liability to attach . . . the defendant must have the right and ability to supervise and control the infringement, not just affect it . . . ."). See also the discussion of the *Visa* case at *supra* notes 29–32 and accompanying text.

and ability to supervise and control the infringement.[126] The court therefore dismissed the vicarious infringement claim.[127]

Conversely, the *Hotfile* court expressly found that Hotfile "had the technology necessary to stop this type of infringement," and therefore had the right and ability to supervise and control the infringement.[128] The different outcome from *Megaupload* was likely caused by a difference in the complaints—while the Film Studios alleged that Hotfile had adequate tools to stop downloads even by unregistered users, Perfect 10 made no such allegation.[129]

On Summary Judgment in *Hotfile*, the Plaintiffs argue that Defendants had the right and ability to unilaterally terminate, suspend, or restrict subscriptions, that they substantially declined to exercise that right, and that the copyrighted content on Hotfile served as a "draw" to consumers.[130] In their Response, Defendants argue that Hotfile cannot practically determine what on their systems is infringing, and point out that Hotfile has no searchable index, that Hotfile users did not have to give their files accurate names like the users in *Napster*, and that "'the system architecture' of Hotfile is not set up to provide Hotfile with the ability to supervise infringing conduct."[131] But, as mentioned above, the gap in search functionality left by Hotfile's strategic decision to leave it out of their site was/is filled by third-party aggregators,[132] in part due to Hotfile's now-abandoned practice of offering and making payments to such aggregators.[133] Further, since uploader-affiliate payments were/are driven by the amount of traffic an uploader lures to her download link, the uploader has a stronger incentive to provide accurate file names (cash),[134] than the users in *Napster*, who were merely motivated by a practical collective interest in files being searchable.[135] Additionally, Hotfile's argument that the architecture of its system does not provide it with the ability to supervise infringing conduct likely triggers the willful blindness doctrine,[136] to be discussed more fully *infra*.

D. Inducement Liability

Perfect 10 did not bring a separate claim for inducement, and the *Grokster* case is not cited in *Megaupload*.[137] The *Hotfile* court cursorily held the allegations that

---

[126] *Megaupload,* No. 11-cv-0191, at 18.

[127] *Id.*

[128] *Hotfile*, 798 F. Supp. 2d 1303, at 1310–11.

[129] *Compare* Megaupload Complaint*, supra* note 74, *with* Hotfile Complaint, *supra* note 82, at ¶23. Without any analysis, the court held that the Studios had adequately alleged that Hotfile profited directly from its failure to exercise its right and ability to control the infringement. *Hotfile*, 798 F. Supp. 2d at 1310.

[130] Hotfile Plaintiffs' Motion for Summary Judgment, *supra* note 62, at 34–35.

[131] Hotfile Defendants' Opposition Memorandum, *supra* note 113, at 32.

[132] *See, e.g., About*, FILESTUBE, www.filestube.com/about.html (last visited Nov. 24, 2012).

[133] See discussion of Hotfile's referral program at *supra* note 89.

[134] See explanation of Hotfile's current and past affiliate programs at *supra* note 90.

[135] A&M Records v. Napster, Inc., 239 F.3d 1004, 1024 (9th Cir. 2001).

[136] *See infra* notes 182–185 and accompanying text.

[137] Perfect 10, Inc. v. Megaupload Ltd.*,* No. 11-cv-0191, 2011 U.S. Dist. LEXIS 81931 (S.D. Cal. 2011).

Hotfile had created a "structured business model that encourages users to commit copyright infringement" sufficient to state a claim for infringement by inducement.[138]

Much of the 72-page indictment against Megaupload is aimed at establishing an inducement-like cause of action—namely, conspiracy to commit willful infringement.[139] In light of the high standard it must meet, the government provides an instructive array of facts which would be significant in establishing an inducement claim. These facts include, to name a few: internal e-mails indicating that Megaupload officials knew that certain uploaders were engaging infringement, and made reward payments to them anyway;[140] internal e-mails transmitting infringing Megaupload links between employees;[141] an internal e-mail instructing employees to ignore large takedown requests unless they come from major sources in the United States, in order to preserve revenue;[142] an e-mail from a third-party advertiser cutting off services which specifically identified infringing Megaupload links;[143] and claims (likely, although not necessarily, supported by screenshot evidence) that specific films and software programs were made publicly available through Megaupload, in some cases at or before their authorized release dates.[144]

The Hotfile Plaintiffs cannot match the evidentiary heft amassed by the U.S. Government, but their case nonetheless has persuasive potential, depending on your view of the facts. Their inducement argument focuses once again on the affiliate program, arguing that Hotfile expressly incentivizes conduct that is more likely to infringe copyrights, while disincentivizing conduct that is less likely to infringe.[145] Plaintiffs also cite to a third-party statement to the effect that Hotfile has a reputation for not suspending or subtracting credits from uploaders that are repeatedly accused of infringement.[146] Further, they claim that Hotfile is used chiefly for infringement, citing a study that found over 90% *of downloads* were infringing.[147] The Plaintiffs even attempt to piggyback on the Megaupload indictment, contending that "defendants modeled Hotfile's business after Megaupload."[148] Additionally, Plaintiffs point out that the Defendants offered technical assistance to users they knew were seeking to infringe copyrights,[149] and refused to implement technology to prevent infringement.[150]

Defendants dispute Plaintiffs' claims on the facts: they argue that the majority of *uploads* to the site are non-infringing,[151] that not one of the Studios' works cracks the top 100 downloads on Hotfile,[152] and that the Plaintiffs' analysis misleadingly

---

[138] *Hotfile*, 2011 U.S. Dist. LEXIS 78387, at *6.
[139] *See* Indictment at 24–52, United States v. Dotcom, No. 1:12CR3 (E.D. Va. Jan. 5, 2012).
[140] *Id.* at 32–33.
[141] *Id.* at 31, 35.
[142] *Id.* at 40.
[143] *Id.* at 34.
[144] *Id.* at 48–50, 52.
[145] Hotfile Plaintiffs' Motion for Summary Judgment, *supra* note 62, at 30.
[146] *Id.* at 30–31.
[147] *Id.* at 31.
[148] *Id.*
[149] *Id.* at 32.
[150] *Id.*
[151] Hotfile Defendants' Opposition Memorandum, *supra* note 113, at 7.
[152] *Id.*

considers only downloads and not all uses of the site.[153] Disclaiming any association with Megaupload, the Defendants claim they modeled their service after Rapidshare, a previously controversial but recently reformed cyberlocker.[154] Hotfile claims that it has taken substantial steps to deter infringement, and that these actions bring it outside of the *Grokster* holding.[155]

There is little disagreement among the parties as to the legal standard applicable to the inducement claim—each side's argument largely follows the factors set out in *Grokster* and marshals the facts to support its claims.[156] Nonetheless, pinning down how a court will weigh the factors relevant to an adjudication of inducement, and how it will interpret the relationship between inducement liability and safe harbor eligibility, remains difficult.[157]

E. Safe Harbor Eligibility[158]

1. Repeat Infringer Policy

Recall that a service provider asserting safe harbor protection as a defense to an infringement claim must first show that it has implemented "a policy that provides for the termination in appropriate circumstances of . . . repeat infringers."[159] This provision is exceedingly vague and raises at least two important issues: (1) what are appropriate circumstances? And (2) if a service provider is under no duty to monitor,[160] what steps can it be required to take to determine the identities of repeat infringers?

The *Hotfile* Plaintiffs argue that the Defendants failed to implement a "meaningful policy to terminate repeat infringers."[161] They note that Hotfile did not cross-reference infringement notices with the uploaders of the noticed files, and did not investigate nor keep track of such users.[162] Further, they use Hotfile's data to quantify how many users accrued 10, 25, 100, or even 300 or more takedown notices

---

[153] *Id.*

[154] *Id.* at 24.

[155] *Id.* at 24–25.

[156] *Compare* Hotfile Plaintiffs' Motion for Summary Judgment, *supra* note 62, at 29–33, *with* Hotfile Defendants' Opposition Memorandum, *supra* note 113, at 23–28.

[157] *See* 6 PATRY, *supra* note 19, § 21.79 (arguing that the scope of *Grokster* inducement liability is indeterminate, and noting a dearth of, and need for, cases which address and develop the theory).

[158] Because Megaupload never got a chance to assert a safe harbor defense in the Perfect 10 lawsuit, and because the question whether the DMCA applies to criminal copyright infringement is complex, novel, and beyond the scope of this Comment, the safe harbor discussion will largely confine itself to the summary judgment briefs in *Hotfile* as well as relevant recent case law. Additionally, § 512(c)(2) conditions eligibility on the service provider's appointment of a registered agent. This Comment eschews analysis of that provision as it raises a pure issue of fact.

[159] 17 U.S.C. § 512(i)(1)(A) (2012).

[160] 17 U.S.C. § 512(m).

[161] Hotfile Plaintiffs' Motion for Summary Judgment, *supra* note 62, at 19–22.

[162] *Id.* at 19–20.

without getting terminated, and estimate that Hotfile paid these users over $10.8 million.[163]

The Defendants admit to documenting only "over 40" terminations from 2009-2011, but respond that the statutory requirement is flexible, that takedown notices are allegations rather than clear indications of infringement, that a "large proportion" of the notices they received were improper, and that Hotfile "continually and proactively strengthen[ed] its policies in response to content owner requests, evolving technology and market shifts."[164]

A consensus appears to be building around the Ninth Circuit's interpretation of the § 512(i)(1)(A) requirement in *Perfect 10 v. CCBill*.[165] There, the court held that a service provider would meet the requirement if it "has a working notification system, a procedure for dealing with DMCA-compliant notifications, and if it does not actively prevent copyright owners from collecting information needed to issue such notifications."[166]

It appears that Hotfile had a procedure for dealing with DMCA-compliant notifications, and that it did not actively hinder content owners from obtaining necessary information. However, Hotfile admits that from 2009-2011, its termination policy was to wait to terminate until a copyright owner sufficiently identified a blatant repeat infringer as such.[167] Significantly, it did not keep track of the users that uploaded noticed files.[168] The court in *CCBill* contemplated that "a substantial failure to record webmasters associated with allegedly infringing websites may raise a genuine issue of material fact as to the implementation of the service provider's repeat infringer policy."[169] Does OCILLA require a content owner both to notify the service provider of specific infringing uses, and to track its notices by user so that it can submit evidence of repeat infringers to the service provider? Or does the § 512(i)(1)(A) requirement place this second obligation – to associate user data with notice data in order to detect repeat infringers – on the service provider?

2. Knowledge

The three-part knowledge requirement is the next hurdle for a webhost asserting safe harbor protection.[170] In *Hotfile*, the Plaintiffs concede that Hotfile responded expeditiously to proper notices of infringement, leaving only actual and "red flag" knowledge in dispute.[171] They make three arguments for their claim that

---

[163] *Id.* at 20. Because the publicly available version of their Motion is redacted, the specific numbers of such users are unavailable at this time.

[164] Hotfile Defendants' Opposition Memorandum, *supra* note 113, at 10–13.

[165] Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1109–11 (9th Cir. 2007); *see also* UMG Recordings, Inc. v. Veoh Networks Inc., 665 F.Supp.2d 1099, 1117 (9th Cir. 2009); Capitol Records, Inc. v. MP3Tunes, LLC, 821 F.Supp.2d 627, 637–38 (S.D.N.Y. 2011).

[166] *CCBill*, 488 F.3d at 1109.

[167] Hotfile Plaintiffs' Motion for Summary Judgment, *supra* note 62, at 11.

[168] *Id.* at 11–12.

[169] 488 F.3d at 1110.

[170] 17 U.S.C. § 512(c)(1)(A) (2012).

[171] *See* Hotfile Plaintiffs' Motion for Summary Judgment, *supra* note 62, at 24–27. Plaintiffs' discussion of the knowledge requirement omits the expeditious response provision entirely. *Id.*

the Defendants had actual knowledge: (1) that, from February to August 2009, Hotfile took down only noticed URLs rather than removing the underlying files from its servers;[172] (2) that service messages from users to Hotfile staff included the download link of the last file the user downloaded-often comprising a word-for-word title of a copyrighted work;[173] and (3) that Hotfile staff actively assisted users in downloading files with "unmistakably infringing titles."[174]

The Defendants respond that the use of a given file at one URL may be infringing while its use at another would not be.[175] Further, they argue that any knowledge they had of file names is irrelevant because file names do not serve as an accurate proxy for infringement.[176]

In *Viacom Int'l Inc. v. YouTube, Inc,* an important recent case determining eligibility for the § 512(c) safe harbor, the Second Circuit distinguished § 512(c)(1)(A)(i) from § 512(c)(1)(A)(ii) as follows: "the actual knowledge provision turns on whether the provider actually or 'subjectively' knew of specific infringement, while the red flag provision turns on whether the provider was subjectively aware of facts that would have made the specific infringement 'objectively' obvious to a reasonable person."[177] This analysis constitutes a departure (though not a wholly drastic one) from a line of cases which had essentially read the red flag provision out of the statute on the basis of legislative history and practical considerations.[178] Though the chances that a service provider will be denied safe harbor protection on a finding of red flag knowledge are still vanishingly small,[179] the courts in *Viacom* and *Shelter Capital*, a recent Ninth Circuit case, have provided two narrow ways a plaintiff could satisfy § 512(c)(1)(A)(ii): First, in *Shelter Capital*, the court suggested in a footnote that a third-party notification of a certain type might constitute a red flag.[180] Second, in *Viacom*, the court held that certain internal e-mails which

---

[172] Hotfile Defendants' Opposition Memorandum, *supra* note 113, at 15.

[173] Hotfile Plaintiffs' Motion for Summary Judgment, *supra* note 62, at 24–25.

[174] *Id.* at 25.

[175] Hotfile Defendants' Opposition Memorandum, *supra* note 113, at 16.

[176] *Id.*

[177] 676 F.3d 19, 31 (2d Cir. 2012).

[178] UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022, 1037 (9th Cir. 2011) (holding Defendant webhost's "general knowledge that it hosted copyrightable material and that its services could be used for infringement . . . insufficient to constitute a red flag."); Capitol Records, Inc. v. MP3Tunes, LLC, 821 F. Supp. 2d 627, 644–45 (S.D.N.Y. 2011); Io Grp., Inc. v Veoh Networks, Inc., 586 F. Supp. 2d 1132, 1148–49 (N.D. Cal. 2008); 3 NIMMER, *supra* note 13, § 12B.04[A][1] (quoting the House Commerce Committee Report, H.R. REP. NO. 105-551(II) at 54 (1998)). *But see* 6 PATRY, *supra* note 19, § 21:85. Professor Patry contrasts the oft-quoted portion of House Commerce Committee Report with a passage from the House Judiciary Committee Report which posits that the § 512(c)(1)(A)(ii) exemption applies as soon as a service provider becomes aware of "information of any kind that a reasonable person would rely upon." *Id.*; H.R. REP. NO. 105-551(I), at 25 (1998).

[179] 3 NIMMER, *supra* note 13, § 12B.04[A][1] (stating that even a "blood crimson" flag would not require investigation or trigger imposition of liability).

[180] 667 F.3d at 1040 n.14.

> A user email informing Veoh of infringing material and specifying its location provides a good example of the distinction [between actual and red flag knowledge]. Although the user's allegations would not give Veoh actual knowledge under § 512(c)(1)(A)(i), because Veoh would have no assurance that a third party who does not hold the copyright in question could know whether the material was infringing, the email could act as a red flag under § 512(c)(1)(A)(ii) provided its information was sufficiently specific.

identified specific infringing works raised a genuine issue of material fact as to YouTube's knowledge both actual and red flag.[181]

3. Willful Blindness

The murky domain of the § 512(c) safe harbor is further clouded by the willful blindness doctrine—which deems that a person has actual knowledge if he "subjectively believe[s] that there is a high probability that a fact exists," and takes "deliberate actions to avoid learning of that fact."[182] Though the Supreme Court has not yet had occasion to apply the willful blindness doctrine in a copyright case,[183] the latest Court of Appeals to speak on the issue—the Second Circuit in *Viacom*—held expressly that "the willful blindness doctrine may be applied, in appropriate circumstances, to demonstrate knowledge or awareness of specific instances of infringement under the DMCA."[184]

4. Financial Benefit, Right and Ability to Control

Finally, a service provider seeking safe harbor must show that it does not receive a financial benefit directly attributable to the infringing activity, in a case in which [it] has the right and ability to control such activity."[185] Here, again, the *Viacom* and *Shelter Capital* decisions are instructive. The district court that heard the *Viacom* case held that "[t]he 'right and ability to control' the activity requires knowledge of it, which must be item-specific."[186] The Ninth Circuit endorsed this view in *Shelter Capital*, stating that "a service provider may, as a general matter, have the legal right and necessary technology to remove infringing content, but until it becomes aware of specific unauthorized material, it cannot exercise its 'power or authority' over the specific infringing item."[187] Significantly, the Second Circuit departed from this reasoning in *Viacom*, noting that making specific knowledge an element of the right and ability to control requirement renders § 512(c)(1)(B) duplicative of § 512(c)(1)(A).[188] But the court offered little guidance to replace the rule it discarded, indicating only that a violation of § 512(c)(1)(B) would likely "involve a service provider exerting substantial influence on the activities of users,

---

Id.

[181] 676 F.3d at 33–34.

[182] Global-Tech Appliances, Inc. v. SEB S.A., 131 S. Ct. 2060, 2070 (2011) (applying the willful blindness doctrine to a patent infringement case).

[183] In *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2006), the Court declined to resolve a conflict between the Ninth and Seventh Circuits with regard to this issue, instead ruling that the evidence in that case supported a finding of actual knowledge. *Global-Tech*, 131 S. Ct. at 2070.

[184] 676 F.3d 19, 40 (2d Cir. 2012).

[185] 17 U.S.C. § 512(c)(1)(B) (2012).

[186] 718 F. Supp. 2d 514, 527.

[187] 667 F.3d 1042.

[188] 676 F.3d at 36.

without necessarily—or even frequently—acquiring knowledge of specific infringing activity."[189]

Curiously, the *Hotfile* Plaintiffs did not argue this point in their Motion for Summary Judgment.[190]

F. Summary: The Current System

One can distill several problems with the current liability scheme from the above cases in the cyberlocker context, and more generally from the case law in the field. The scope of a service provider's liability for secondary infringement,[191] and to a lesser extent, for direct infringement,[192] is unclear and defined by manipulable standards. The limits of the safe harbor provided by § 512(c) are similarly muddled.[193] Furthermore, the structure and practice of the notice and takedown system gives counterproductive incentives to all parties:

Service providers are discouraged from filtering uploaded content prior to notification of infringement,[194] and directed to take down whatever a copyright owner decides is infringing, with little practical safeguards for users' interests.[195]

Copyright owners, assured of cooperation and aware that the consequences of misuse on their part are negligible,[196] have every incentive to exploit the procedure in an overprotective manner.[197]

---

[189] *Id.* at 47–48.

[190] Hotfile Plaintiffs' Motion for Summary Judgment, *supra* note 62, at 19–27. The Plaintiffs' OCILLA argument does not include any analysis of the financial benefit/right and ability to control provision. *Id.*

[191] *See* Lital Helman, *Pull Too Hard and the Rope May Break: On the Secondary Liability of Technology Providers for Copyright Infringement*, 19 TEX. INTELL. PROP. L. J. 111, 131 (2010) ("The open-ended nature of the secondary liability standard renders it difficult, if not impossible, to predict the results of future cases or even the theories upon which they would be decided.").

[192] *See supra* notes 13–18, 94–105 and accompanying text.

[193] *Compare* Columbia Pictures Indus., Inc. v. Fung, 96 U.S.P.Q.2D (BNA) 1620 (C.D. Cal. 2009) (holding, in a case where the defendant did not have a viable safe harbor defense, that an online service that meets the *Grokster* standard *may not* assert a safe harbor defense), *with* Viacom Int'l Inc. v. YouTube, Inc., 718 F. Supp. 2d 514, 526 (S.D.N.Y. 2010) (distinguishing *Fung* and holding that *Grokster* inducement does not apply to cases where safe harbor protection is warranted).

[194] *See Viacom*, 718 F. Supp. 2d at 525. Since complying with the statutory requirements after notification exempts a webhost from liability, there is arguably little incentive to incur the cost of filtering. *Id.* Furthermore, filtering may be an indication of ability to control infringement, exempting the service provider from safe harbor protection under 17 U.S.C. § 512(c)(1)(B). Tur v. Youtube, Inc., 2007 U.S. Dist. LEXIS 50254 (C.D. Cal. June 20, 2007) ("the requirement presupposes some antecedent ability to limit or filter copyrighted material"). *But see* Ginsburg, *supra* note 6, at 587 (arguing that sites may have an interest in filtering to promote the perception of legitimacy) *and* Tim Wu, *The Copyright Paradox*, 2005 SUP. CT. REV. 229, 247 (contending that under *Grokster*, filtering may give rise to a presumption of intent not to induce).

[195] *See* Edward Lee, *Decoding the DMCA Safe Harbors*, 32 COLUM. J. L. & ARTS 233, 234–35 (2009). Again, since complying with the statutory requirements exempts the host from liability, it has a strong incentive to take down whatever material is referenced in the notice without taking the time to assess whether the copyright is in fact owned by the party giving notice or whether the material does in fact infringe.

Copyright owners have complete information about the files being infringed and a direct interest in protecting against infringement, while service providers have greater access to and control over uploaded files. Congress intended OCILLA to serve as a compromise between these two principal categories of stakeholders, but in the context of cyberlockers and other § 512(c) technologies, the current system saddles copyright owners with a disproportionate share of the burden to enforce the copyright law.

III. PROPOSAL

With these problems in mind, commentators, legislators, and industry stakeholders have proposed numerous alternative methods of promoting responsible copyright enforcement without encroaching on free speech rights or the free flow of information. This section will survey four such proposals and argue for a solution that incorporates aspects of each of them.

A. The "Follow the Money" Approach

Both Houses of Congress recently considered legislation to regulate digital piracy.[198] The Protect IP Act (PIPA), introduced in the Senate in May 2011, and the Stop Online Piracy Act (SOPA), introduced in the House of Representatives in October 2011, would have left the current liability system intact, but attempted to improve enforcement by providing additional remedies to content owners and to the Attorney General.[199]

Under the bills, if a court determined that a site was dedicated to infringement, it could have ordered: (1) internet service providers to block public access to the site; (2) payment system providers to suspend or terminate service to the site; (3) advertising services to suspend or terminate service to the site; and (4) search engines to disable links to the site.[200] In both bills, the first (and most drastic) of these restrictions was only applicable to foreign sites that did business in the U.S.,

---

[196] *See* Lenz v. Universal Music Corp., 572 F. Supp. 2d 1150, 1156–57 (N.D. Cal. 2008) (holding copyright owner liable under 17 U.S.C. § 512(f) for misusing the takedown procedure by issuing a takedown notice without considering whether the uploaded material had a fair use defense, but anticipating that damages would be nominal).

[197] *See Megaupload*, 2011 U.S. Dist. LEXIS 81931 at *14–15 (describing Perfect 10's submission of 22 takedown notices, only one of which actually referred to material for which it owned the copyright); *MP3Tunes*, 2011 U.S. Dist. LEXIS 93351 at *14 (discussing a takedown notice sent by EMI requesting removal of all EMI copyrighted works based on the "representative list" it had provided).

[198] Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011, S. 968, 112th Cong.; Stop Online Piracy Act of 2011, H.R. 3261, 112th Cong.

[199] H.R. 3261 § 2(a)(2) ("Nothing in Title I [which includes §§ 102 and 103] shall be construed to enlarge or diminish liability, including vicarious or contributory liability, for any cause of action available under title 17, United States Code, including any limitations on liability under such title."); *see also* Terrence Hart, *SOPA: New Remedies for Existing Liability*, COPYHYPE (Nov. 14, 2011) http://www.copyhype.com/2011/11/sopa-new-remedies-for-existing-liability/.

[200] S. 968 §§ 3–4; H.R. 3261 §§ 102–103.

and could only be sought in an action by the Attorney General.[201] Though that element of the legislation was heavily backed by the content industry,[202] it was abandoned prior to the online protests; the bills that were eventually tabled included only the last three, more indirect measures.[203]

As noted above, the requirements for establishing liability under the bills tracked those of existing secondary liability law. In its final form, SOPA provided two definitions of the term "site dedicated to theft of U.S. Property:"[204] (1) the site is primarily designed, operated, or marketed for, or has "only limited purpose or use other than" copyright and/or trademark infringement;[205] or (2) the operator of the site "promotes its use" for infringement.[206] The first definition can be characterized as a stronger version of the *Sony* standard, and the second as a codification of *Grokster*.[207]

---

[201] S. 968 §§ 2(9), 3; H.R. 3261 § 102. There is much debate as to whether the collateral negative consequences (chiefly due process, free speech, and national reputation concerns) of Domain Name System (DNS) filtering outweigh its potential effectiveness. *Compare* Mark A. Lemley, David S. Levine & David G. Post, *Don't Break the Internet* (Jan. 3, 2012), 64 STANFORD L. REV. ONLINE 34, Dec. 2011., *available at* http://ssrn.com/abstract=1978989 (positing that DNS filtering is ineffective and would result in significant and pervasive collateral damage), *with* George Ou, *My Filtering Research Before the House SOPA Panel*, HIGH TECH F. (Dec. 16, 2011), http://www.hightechforum.org/my-dns-filtering-research-before-house-sopa-panel/ (rebutting arguments that DNS filtering would harm DNSSEC, and arguing that filtering would target piracy with limited collateral damage).

[202] Michael O'Leary, News Release, Motion Picture Association of America (Jan. 12, 2012) *available at* http://www.wired.com/images_blogs/threatlevel/2012/01/olearystatement.pdf ("We continue to believe that DNS filtering is an important tool, already used in numerous countries internationally to protect consumers and the intellectual property of businesses with targeted filters for rogue sites").

[203] Eric Engleman, *Leahy Floats Change to Senate Version of Hollywood-Backed Anti-Piracy Bill*, BLOOMBERG NEWS (Jan. 13, 2012) http://www.bloomberg.com/news/2012-01-12/senator-leahy-proposes-change-to-hollywood-backed-anti-piracy-measure.html (reporting that a key sponsor of the Protect IP Act planned to propose an amendment requiring the DNS filtering provision "to be studied before it is implemented"); News Release, Office of Congressman Lamar Smith (Jan. 13, 2012), http://judiciary.house.gov/news/DNS%20blocking%20SOPA.html ("[Lamar Smith, the Chairman of the House Judiciary Committee] feel[s] we should remove Domain Name System blocking from the *Stop Online Piracy Act* so that the Committee can further examine the issues surrounding this provision.").

[204] A December Manager's Amendment eliminated a third definition that was present in the original bill. *Compare* H.R. 3261, 112th Cong. § 103(a)(1)(B)(ii)(I) (as introduced, October 26, 2011), *with* H.R. 3261, 112th Cong. § 103(a)(1)(C)(ii) (as amended, December 12, 2011). This third definition essentially codified the willful blindness doctrine most notably applied in the context of digital copyright law by the Seventh Circuit in the *Aimster* case. 334 F.3d 643, 650 (2003).

[205] H.R. 3261 § 103(a)(1)(C)(i).

> the site is primarily designed or operated for the purpose of, has only limited purpose or use other than, or is marketed by its operator or another acting in concert with that operator primarily for use in, offering goods or services in violation of [in pertinent part, 17 U.S.C. § 501 which covers civil infringement of copyright].

Id.

[206] *Id.* at § 103(a)(1)(C)(ii) ("[T]he operator of the site operates the site with the object of promoting, or has promoted, its use to carry out acts that constitute a [copyright infringement], as shown by clear expression or other affirmative steps taken to foster such violation").

[207] Hart, *supra* note 199; *compare Sony*, 464 U.S. 417, 442 ("capable of commercially significant non-infringing use"), *with Sony*, 464 U.S. 417, 491 (Blackmun, J., dissenting) ("[I]f a *significant* portion of the product's use is *noninfringing*, the manufacturers and sellers cannot be held

In a recent working paper, Professor David G. Robinson argues from successful use of intermediary regulations in several analogous contexts that such measures would have similar success if applied to digital copyright and trademark piracy.[208] In particular, Professor Robinson cites the success of the payment system provisions of the Unlawful Internet Gambling Enforcement Act of 2006 (UIGEA)[209] as indicating that similar provisions would likely work in the copyright context.[210] But there are key differences between internet gambling and online copyright infringement that weaken this argument.[211] While SOPA/PIPA would enhance enforcement of copyright law against the most egregious offenders (the bills' principal targets), in close cases like *MP3Tunes* they would suffer from the same infirmities as the existing system.

B. Graduated Response

Faced with high costs and uncertain outcomes when litigating against service providers, a public relations nightmare when litigating against users, and an inability to secure legislative amendments to the DMCA, the content industry has shifted in recent years to a strategy termed "graduated response."[212] This approach

---

contributorily liable for the product's infringing uses.") (emphasis in original); *see also Grokster*, 545 U.S. 913, 936–37 ("[O]ne who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties").

[208] David G. Robinson, *Following the Money: A Better Way Forward on the Protect IP Act* (Sept. 18, 2011), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1930013. Professor Robinson surveys the success of both voluntary and legally compelled actions taken by payment service providers against illegal online tobacco sales, child pornography, online pharmacies, and internet gambling. *Id.* at 16–18.

[209] 31 U.S.C. §§ 5361–67 (2012).

[210] *Id.* § 5364; Robinson, *supra* note 208, at 18–19. Estimates suggest that the UIGEA decreased the value of online casino gambling businesses by up to 80 percent. *Id.* at 19.

[211] The UIGEA requires financial institutions to maintain the coding and blocking systems most of them had in place prior to the act. 31 U.S.C. § 5364(c). These systems are based on the merchant category code—each business tags its credit card sales with a four-digit code that represents the category of good or service sold. Mark MacCarthy, *What Payment Intermediaries are Doing About Online Liability and Why it Matters*, 25 BERKELEY TECH. L.J. 1037, 1062–65 (2010). Gambling has its own code, and internet transactions are marked with an electronic commerce indicator, so a financial institution simply blocks transactions marked with both the code and the indicator in jurisdictions that don't allow internet gambling, and processes such transactions as normal in jurisdictions that permit internet gambling. *Id.* at 1062–1063. Further, the institutions routinely run test transactions to ensure that merchants are properly coding. *Id.* at 1064. The system is effective, but overinclusive,—it runs into significant problems when some of the transactions that would be coded as gambling are illegal in a given jurisdiction, while others are not. *Id*. at 1072. In contrast, membership fees for cyberlockers could not be coded in the same way as gambling transactions, and even if they could, such a system would be too overinclusive to be justified. In SOPA/PIPA, the payment systems provisions operated much less comprehensively—they could only be invoked against specific sites that were adjudicated to be dedicated to infringing use. H.R. 3261 § 103(a), 103(b)(1); S. 968 § 4(a)(1), 4(d)(2)(a). Since the two legislative schemes would be markedly different, it is difficult to argue from the success of the UIGEA to the success of the payment provisions of SOPA/PIPA.

[212] *See generally* Annemarie Bridy, *Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement*, 89 OR. L. REV. 81 (2010).

focuses on education, with the goal of inducing casual users of pirated content to seek out legal alternatives.[213] In July of 2011, a large consortium of major copyright owners (including the MPAA, the RIAA, and their members) teamed up with a group of major service providers (including Comcast, TimeWarner Cable, Verizon, AT&T, and Cablevision) to create the Center for Copyright Information ("CCI"), which will administer the newly created "Copyright Alert System" ("CAS").[214] The system requires ISPs to send up to six notices to users accused of infringement by copyright owners.[215] Though implementation of the CAS has been delayed, CCI's Executive Director recently confirmed that the system would be online in the near future.[216]

France's controversial HADOPI Law, passed in 2009, is perhaps the most well-known example of a graduated response system.[217] In contrast to the CAS, HADOPI is a mandatory, statutory regime, administered by a government agency.[218] Rather than six notices and a decrease in service speed, HADOPI provides that a repeat offender may be disconnected from internet access altogether after three notices.[219] Though empirical evidence suggests that the program has been at least moderately

---

[213] CENTER FOR COPYRIGHT INFORMATION, MEMORANDUM OF UNDERSTANDING at 1 (2011), *available at* http://www.copyrightinformation.org/sites/default/files/Momorandum%20of%20Understanding.pdf.

[214] *Id.* at 3.

[215] *Id.* at 8–13. The system comprises four steps: (1) an initial educational step, in which the ISP sends up to two notices explaining that a content owner has complained of the user's conduct, and giving information about the nature and effects of online infringement; (2) an acknowledgment step, in which the ISP sends up to two more notices which require the user to acknowledge receipt and agree to cease infringing before she can access the internet; (3) a mitigation measures step, in which the ISP sends another notice to the user, this time incorporating all elements of the educational acknowledgment notices, as well as informing the user that the ISP will take one of several mitigation measures if the user does not seek an administrative review (administered by the American Arbitration Association). The mitigation measures include temporarily downgrading the speed of the user's service in a number of different ways, temporarily directing the user to an educational landing page every time she connects to the internet, and temporarily restricting the user's internet access; and (4) a post mitigation measures step in which the ISP informs the user that she may be subject to a lawsuit for copyright infringement and/or imposes additional or alternative mitigation measures. *Id.* at 10–13.

[216] Jill Lesser, *The Copyright Alert System: Moving to Implementation*, CENTER FOR COPYRIGHT INFO. (Oct. 18, 2012), http://www.copyrightinformation.org/node/709.

[217] Nathan Lovejoy, *Procedural Concerns with the HADOPI Graduated Response Model*, JOLT DIGEST (Jan. 13, 2011, 10:16 PM), http://jolt.law.harvard.edu/digest/copyright/procedural-concerns-with-the-hadopi-graduated-response-model (characterizing HADOPI as "the most prominent example of the legislative-backed graduated response schemes").

[218] Loi 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur Internet [Law 2009-669 of June 12, 2009 promoting the diffusion and protection of creation on the Internet], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], June 13, 2009, p. 9666.

[219] Alain Strowel, *Internet Piracy as a Wake-up Call for Copyright Law Makers – Is the "Graduated Response" a Good Reply?*, 1 W.I.P.O.J. 75, 80 (2009).

successful,[220] the newly elected French Government plans to significantly decrease funding to HADOPI, arguing that its costs outweigh its benefits.[221]

Importantly, graduated response systems raise significant issues regarding the rights of users.[222] Many of these issues are tied to the scheme in general—if law and practice incentivize copyright owners to err on the side of overprotection, a simple graduated response system just adds more ways for them to assert their ownership rights erroneously, infringing on users' rights to substantive due process, free speech, and privacy.

C. The Best Available Technology Standard

In an important recent article, Lital Helman and Gideon Parchomovsky have proposed a comprehensive solution to the problems the existing legal framework poses for online service providers and copyright owners alike.[223] By making filtering of uploaded content prior to notification of infringement a prerequisite for safe harbor protection, they argue, Congress could bring clarity and predictability to the field, and give all parties strong incentives to eradicate infringement without crippling innovation or chilling speech.[224]

Helman and Parchomovsky's "best available technology" standard adds a pre-notification requirement to the existing notice and takedown procedure,—a service provider must filter uploaded content using a technology that meets current standards.[225] The proposed system would include a single database,[226] in which copyright owners would deposit information about the legal status of their works.[227]

---

[220] *See* Glenn Peoples, *Can Copyright Alerts Work in U.S.? Hadopi Report Brings Promising Signs*, BILLBOARD.BIZ (Oct. 29, 2012), http://www.billboard.biz/bbbiz/industry/legal-and-management/business-matters-can-copyright-alerts-work-1007993712.story. Peoples cites recent reports and studies which indicate that, since passage of the law, recipients of notices have tended to refrain from infringing, peer-peer traffic has decreased, and digital sales have increased. *Id.*

[221] Bruce Crumley, *Why France's Socialists Won't Kill Sarkozy's Internet Piracy Law*, TIME MAG. (Aug. 2, 2012), http://world.time.com/2012/08/02/why-frances-socialists-wont-fully-kill-off-sarkozys-internet-piracy-law/.

[222] *See* Peter K. Yu, *The Graduated Response*, 62 FLA. L. REV. 1373, 1394–1403 (2010).

[223] Lital Helman & Gideon Parchomovsky, *The Best Available Technology Standard*, 111 COLUM. L. REV. 1194 (2011).

[224] *Id.* at 1197. Helman and Parchomovsky argue that, on top of encouraging webhosts to implement anti-infringement filtering technology, their new scheme would "serve as a constant spur for technology companies to improve existing filtering technologies toward more accurate identification and removal of infringing content on the one hand, and retention of noninfringing content on the other." *Id.*

[225] *Id.* at 1217. The best available technology is defined as "the technology that offers the best effectiveness/cost ratio," where effectiveness is defined as the ratio of infringing works blocked to non-infringing works blocked. *Id.* at 1218. False positives and false negatives are treated equally, because "developers of filtering mechanisms should have an equal incentive to invest in minimizing both types of mistakes." *Id.* at 1218–19.

[226] *Id.* at 1221. The database would be created under the supervision of either the Copyright Office or a private body akin to the Internet Corporation for Assigned Names and Numbers (ICANN), which administers domain names. *Id.* at 1222.

[227] *Id.* at 1219–22. This would give each filtering system the ability to check uploaded files against every registered copyrighted work without having to go from copyright owner to copyright owner to track down the relevant information. *Id.*

Because filtering displays economies of scale, the proposal also calls for the establishment of several competitive clearinghouses to provide filtering services for webhosts.[228] An agency, either independent or under the auspices of the Copyright Office, would maintain a list of the best available filtering technologies.[229] To avoid liability, a website proprietor would need only show that the filter employed by the site (or by its commissioned clearinghouse) was on the list at the time of the alleged infringement.[230]

At bottom, two key considerations inform this proposal. First, websites that host user content are better situated to detect infringing uploads than copyright owners, because websites already control their own systems.[231] Second, pre-notification enforcement, if effective, would substantially diminish the need for costly litigation by introducing legal certainty.[232]

Professors Sonia Katyal and Jason Schultz recently responded critically to Helman and Parchomovsky's proposal.[233] Katyal and Schultz argue that the best available technology standard would benefit an unproven industry (content filtration) at the expense of "proven drivers of economic growth" (web services and content dissemination industries).[234] They challenge Helman and Parchomovsky's assumption that the costs of copyright-owner enforcement are prohibitive.[235] Further, they contend that shifting filtering responsibility to service providers could have significant negative effects on the performance of their services and the internet at large.[236] Moreover, Katyal and Schultz question the capacity of automated filters to adequately account for fair use and other complicating aspects of the modern infringement determination,[237] and contend that Helman and Parchomovsky fail to adequately address due process[238] and free speech concerns.[239]

---

[228] *Id.* at 1215–16. Filtering systems are expensive to install, update, and maintain, but the cost of each upload is constant and low. *Id.* at 1215. Competition among clearinghouses provides a strong incentive both to the clearinghouses themselves and to developers of filtering technology to improve the quality and efficiency of their filtering services. *Id.* at 1216.

[229] *Id.* at 1224–25. The agency would update the list periodically, and filtering centers whose technology had become outdated would be given a reasonable time to update their systems. *Id.* at 1236.

[230] *Id.* at 1236.

[231] *Id.* at 1213. To implement an effective filtering system, a party must have two things: (1) a list of files to compare against the uploads, and (2) access to the system whose uploads are being filtered. *Id.* As a practical matter, it is far more plausible to require copyright owners to deposit their information in a database accessible to service providers than it is to require service providers to provide access to their system to every copyright owner. *Id.* at 1213–14.

[232] *Id.* at 1227–28. Since the proposal clarifies and ensures application of safe harbor protection to online service providers that follow procedures to filter uploads to their sites, a copyright owner would be unwise to bring a lawsuit against such a service provider. *Id.* at 1227.

[233] Sonia Katyal & Jason Schultz, *The Unending Search for the Optimal Infringement Filter*, 112 COLUM. L. REV. SIDEBAR 83 (2012).

[234] *Id.* at 88.

[235] *Id.* at 90.

[236] *Id.* at 91.

[237] *Id.* at 96–101.

[238] *Id.* at 102–104.

[239] *Id.* at 104–106.

D. Digital Fingerprinting as a Standard Technical Measure

What if a workable filtering requirement could be achieved without additional legislation? As noted *supra*, OCILLA requires all service providers to "accommodate and . . . not interfere with standard technical measures."[240] In a recent article, Lauren Gallo argues that this provision could support a filtering requirement because digital fingerprinting technology meets the statutory definition of a standard technical measure.[241] Digital fingerprinting services work by extracting identifying features from digital files to create a profile that can be checked against a database of other such profiles.[242] Recall that under the statute a standard technical measure must be relatively inexpensive, reasonably available, "used by copyright owners to identify or protect copyrighted works," and developed pursuant to a broad consensus of copyright owners and service providers.[243]

It is self-evident that copyright owners use digital fingerprinting technology to identify copyrighted works. Audible Magic, a leader in the copyright filtering industry, scales its pricing based on volume of upload, even offering its service at no cost to low-volume customers.[244] This example demonstrates a likelihood that digital fingerprinting satisfies the cost and availability requirements. That leaves the question of broad consensus.

In 2007, a group of copyright owners and media companies came together to adopt the User Generated Content Principles ("UGC Principles"), a voluntary agreement which, in most pertinent part, imposes on user generated content services an unenforceable requirement that they implement commercially reasonable content identification technology.[245] In the years following adoption of the UGC Principles, large numbers of content owners and service providers have implemented digital fingerprinting technology.[246] Ms. Gallo argues that these two constituencies should acknowledge that the required consensus has been reached.[247]

---

[240] 17 U.S.C. § 512(i)(1)(B) (2012).

[241] Lauren G. Gallo, Note, *The (Im)Possibility of "Standard Technical Measures" for UGC Websites*, 34 COLUM. J.L. & ARTS 283, 284 (2011).

[242] *See* MEDIAHEDGE, DIGITAL FINGERPRINTING WHITE PAPER at 5 (2010), *available at* http://www.mediahedge.com/fileadmin/bestanden/pdf/White_Paper_-_Digital_Fingerprinting_by_Mediahedge_01-2010.pdf.

[243] 17 U.S.C. § 512(i)(2).

[244] *Copyright Compliance*, AUDIBLE MAGIC, http://audiblemagic.com/solutions-compliance.php (last visited Nov. 26, 2012).

[245] Press Release, User Generated Content Coalition, Internet and Media Industry Leaders Unveil Principles to Foster Online Innovation While Protecting Copyrights (Oct. 18, 2007), http://www.ugcprinciples.com/press_release.html; *Principles for User Generated Content Services*, http://www.ugcprinciples.com/ (last visited Nov. 26, 2012).

[246] *See SmartID Customers & Partners*, AUDIBLE MAGIC, http://www.audiblemagic.com/customers-contentid.php (last visited Nov. 26, 2012) (listing 47 webhost-clients including facebook, Microsoft, myspace, and Verizon); *Content Owners*, AUDIBLE MAGIC, http://audiblemagic.com/customers-contentregistration.php (last visited Nov. 26, 2012) (listing 20 content owner-clients including Disney, NBC Universal, and Viacom); *Clients*, CIVOLUTION, http://www.civolution.com/clients-and-partners/clients/ (listing 39 clients); *Content ID,* YOUTUBE, http://www.youtube.com/t/contentid (last visited Nov. 26, 2012) (explaining YouTube's comprehensive digital fingerprinting system).

[247] Gallo, *supra* note 241, at 314–15.

In response to the UGC Principles, the Electronic Frontier Foundation ("EFF") and a group of non-profit organizations propounded their Fair Use Principles for User Generated Video Content.[248] Among other things, the Principles would require a showing that 90% or more of the source file be present in order for a file to be blocked.[249] Such a requirement would do much to protect fair use, but would be ripe for abuse via token compliance—a user could post 89% of a given work in a blatantly infringing manner, and the copyright owner would have no recourse. Additionally, requiring webhosts to check full uploaded files against full source material files would saddle them with an undue burden.

E. A Comprehensive Policy for Online Infringement Reduction

The emergence of cyberlockers is one of many recent trends demonstrating that the current legal framework permits business plans that promote and indeed rely on infringement, while flouting the due process and free speech rights of users. The OCILLA is failing to achieve its purposes. Significant changes are necessary.

The best available technology proposal and the standard technical measure proposal both rightly point to the need for universal use of filtering technology. Their duty to filter is a bright line intent requirement that clarifies the *Grokster* rule's application by making intent a binary issue.[250] It is more efficient than an actual intent requirement because it represents a brighter line—not only is intent analyzed, but the specific method of proving intent is enumerated. Further, their filtering requirement would deter online storage providers from technically complying with OCILLA while allowing, or relying on, mass infringement.

But how would these filters take account of fair use and other defenses? Helman and Parchomovsky argue that filters are likely to get better at detecting fair use through effective use of quantitative proxies, and that they could be supplemented by human review.[251] Because fair use is a necessarily flexible doctrine on which even reasonable judges, scholars, and lawyers disagree, it is almost self-evident that the ideal of an automated filter that sufficiently addresses fair use in all cases is practically unattainable.[252]

Katyal and Schultz argue that the inability of technology to reliably address factual questions of copyright infringement, or to properly protect the due process and free speech rights of users, counsels in favor of maintaining the current system.[253] Further, they question "whether a system involving both filtering and

---

[248] *Fair Use Principles for User Generated Video Content*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/pages/fair-use-principles-user-generated-video-content (last visited Nov. 26, 2012).

[249] *Id.*

[250] *See* Ginsburg, *supra* note 6, at 586–88. Professor Ginsburg points out that the *Grokster* decision was unclear as to whether the combination of a failure to filter and a business plan that benefits from infringement would suffice to establish liability. *Id.*

[251] Helman & Parchomovsky, *supra* note 223, at 1229–32.

[252] *See* Pamela Samuelson, *Unbundling Fair Uses*, 77 FORDHAM L. REV. 2537, 2543 n.37 (2009) ("Particularly in close fair use cases, judges are likely to differ in their predisposition to err in favor or against fair use defenses; some inconsistency in fair use case law is inevitable.").

[253] Katyal & Schultz, *supra* note 233, at 100.

human review would be any more efficient than the current one."[254] But the current system has incentivized webhosts to adopt (imperfect) filtering technology in ways that also raise substantial due process and free speech concerns.[255] A new system which combines mandated filtering with meaningful protections for users' rights is in order.

Because a filter is unlikely to account meaningfully for qualitative considerations, the system should employ quantitative proxies to efficiently dispose of the easy cases. Because quantitative proxies will necessarily get closer cases wrong, the automated system must be supplemented by human review. Such an arrangement reduces costs by directing expensive human review to the close cases where it is indispensable. Furthermore, in the extreme case where a webhost builds its business on obvious infringement, copyright owners should be provided with effective legal remedies which afford adequate due process.

This author proposes that, in lieu of an (unlikely) express private agreement or legislative enactment, courts begin holding that digital fingerprinting qualifies as a standard technical measure under § 512(i). The interested parties—mass content owners, webhosts, and consumer groups—should then form a non-profit standards organization (hereinafter Digital Copyright Standards Organization – "DCSO") to implement an efficient review system that would equitably allocate the costs of necessary infringement determinations.

To account for fair use and other defenses, and to more adequately address due process concerns, a "filter-and-review" system would be instituted. The system would implement a "X% of the fingerprint" rule. That is, only files incorporating more than, say, 90% of a protected fingerprint would be subject to automatic blocking. In that situation, the uploading user would be entitled to pursue administrative review. Further, the webhost would be required to keep track of uploads that contain less than 90%, but more than, say, 60%, of the underlying fingerprint. Files in this second category would be tabulated both by user and by work: So, if for example a user of a given site uploaded a file containing 60% or more of a protected fingerprint, the webhost would be required to notify that user that her upload contained an unusually large proportion of copyrighted material according to the site's filter. After ten such uploads, each of the uploads would be blocked. The user would have a right to administrative review regarding any or all of the subject uploads after receiving notice. That process would also become available to a copyright owner if users uploaded files containing 60% or more of a given work's fingerprint to a given site five times or more.

Because this new regime would operate under § 512(i) and would not displace the notice and takedown provisions, a copyright owner could seek removal of any alleged infringement not detected by the new scheme by filing a regular notice pursuant to § 512(c)(3).

---

[254] *Id.*

[255] *See* Ke Steven Wan, *Managing Peer-to-Peer Traffic with Digital Fingerprinting and Digital Watermarking*, 41 SW. L.J. 331, 345–47 (2012). Professor Wan argues that the notice and takedown provisions fail to provide adequate recourse to users with credible defenses, and chill free speech by giving webhosts strong incentives to forego analysis and merely take down every file about which they receive a notice. *Id.*

The proposed administrative review process could loosely follow the framework of the Uniform Domain Name Dispute Resolution Policy ("UDRP")[256] with important changes. Briefly, the UDRP establishes an administrative review process for disputes over domain names that allegedly infringe trademarks.[257] Each owner of a domain name agrees to submit to the process as part of the registration agreement for the domain name.[258] The complaining trademark owner selects the provider of arbitration services from a list of approved providers.[259] After a panel of one or three arbitrators is appointed, the panel reviews the submissions of each party and enters a decision within fourteen days.[260]

The proposed DCSO would also approve a set of dispute resolution service providers, but unlike the UDRP, it would dictate random selection of the provider in each case. Next, the provider would arrange for an administrative arbitrator, or, at the election of either party, an administrative panel of three, to hear the case. Finally, the arbitrator or panel would accept evidence from both parties, and submit its decision within fourteen days. Because costs would need to be low enough to ensure broad access to the review process, but not so low as to encourage frivolous challenges, the author proposes that content owners and webhosts jointly contribute to a subsidy fund, and that the remaining cost of a given dispute be borne by the losing party.

Further, the author proposes incorporating the least controversial remedies set forth in SOPA/PIPA—cessation of services from payment systems and advertisers. The availability of these remedies would enhance enforcement both in the transition phase and after the new scheme is implemented. Indeed, the proposed system would facilitate the administration of these remedies, because brazen failure to adopt an approved filtering system would provide clear cause for invoking them.

Lastly, a voluntary graduated response system like the CAS would supplement these measures by educating users and promoting legal alternatives to piracy.

CONCLUSION

In sum, the ascent of cyberlockers is one of many significant challenges to the current legal framework surrounding online protection of copyrighted work. To date, courts' attempts to discern and apply vague doctrines and inconsistent precedents in the context of this burgeoning technology have yielded uncertainty for all parties.

It would be naïve to expect that Internet piracy could somehow be completely eradicated. Like alcohol and drug abuse, these practices will surely continue regardless of the level at which they are regulated. But we can still do better than we are doing right now. A new filtering scheme that provides a clear exemption from liability conditioned on adoption of pre-notification anti-infringement measures

---

[256] *Uniform Domain-Name Dispute-Resolution Policy*, INTERNET CORP. FOR ASSIGNED NAMES AND NUMBERS (Oct. 24, 1999), http://www.icann.org/en/help/dndr/udrp/policy.

[257] *Id.* at (1).

[258] *Id.*

[259] *Id.* at (4)(d).

[260] *Rules for Uniform Domain Name Dispute Resolution Policy* (15)(b), INTERNET CORP. FOR ASSIGNED NAMES AND NUMBERS (Oct. 30, 2009), http://www.icann.org/en/help/dndr/udrp/rules.

would replace murky standards with clarity and produce effective copyright enforcement naturally, by way of economic incentives. The changes proposed in this article are designed to emphasize the importance of a multi-faceted approach to the complex problems presented by online copyright infringement, and to sketch the form such an approach might take.