MEGA, DIGITAL STORAGE LOCKERS, AND THE DMCA: WILL INNOVATION BE STIFLED BY FEARS OF PIRACY?

ALI V. MIRSAIDI [†]

ABSTRACT

Kim Dotcom, founder of Megaupload Limited, has been in many news headlines over the past year. Megaupload—one of Dotcom's many peer-to-peer sharing sites—was the center of controversy, as it allowed users to upload and share all sorts of files, including copyrighted material. After an organized effort by the Department of Justice and several foreign governments, Dotcom was arrested for (secondary) copyright infringement and his site was ultimately shut down.

Dotcom has recently launched a new service, MEGA, which he claims will evade copyright laws entirely. Like other well-known cloud-sharing services such as Dropbox and Google Drive, MEGA allows users to upload files and to share them with select users. In an attempt to avoid liability, MEGA locally encrypts all files on the user's computer before they are uploaded to the site. The private key and public key used to encrypt and decrypt the file are retained solely by the user; MEGA gets no part of that information. This, Dotcom argues, will shift the entirety of the copyright onus to the user.

This Issue Brief analyzes the protections afforded cyberlocker services like MEGA by the DMCA, including tensions raised in actual litigation. This Issue Brief argues that, while an ex ante *secondary-liability analysis is difficult due to its contextual nature, MEGA's use of user-controlled encryption (UCE), deduplication, and distributed host servers may lend to an affirmative finding of liability.*

INTRODUCTION

The advance of technology has presented new difficulties in the interpretation and application of copyright law. The most problematic advances are those that have brought copyright infringement to the masses.

[†] Duke University School of Law, J.D. 2014; Stony Brook University, B.S. Computer Science and Applied Mathematics 2008. I would like thank the journal's wonderful editors for their comments and feedback.

Proprietors of such technologies can distribute devices or provide services that have the capability to infringe copyright, without directly infringing themselves and thereby evading copyright liability. To address this problem, courts have fashioned secondary liability to impose liability on these individuals.

Most recently, peer-to-peer (P2P) services have come under scrutiny because they allow third-party users to infringe copyright without directly involving the service provider in that infringement. Such technologies include Napster, Grokster, Morpheus, and Limewire, among others. Although the law has developed around these P2P services,[1] a new type of technology has emerged that could test the metes and bounds of this judge-made law: digital storage lockers, also known as cyberlockers. Cyberlockers allow users to store files in the cloud,[2] either for personal use or to be distributed to other users. Cyberlockers do not employ any filtering mechanisms. Rather, users are able to upload and share whatever material they choose—including potentially copyrighted material.

Among the newest of these is Kim Dotcom's MEGA cyberlocker.[3] Dotcom gained Internet notoriety through the rise and fall of his earlier cyberlocker service, Megaupload.[4] Allegedly accounting for 4 percent of total Internet traffic,[5] the site was shut down by the U.S. Department of Justice in early 2012.[6] Although copyright-infringement charges have been brought against Dotcom,[7] he has nonetheless launched a new cyberlocker service, MEGA.[8] Unlike its previous iteration, the new MEGA site offers several key features: user-controlled encryption, deduplication, and distributed hosting.[9] Although all cyberlockers employ some form of

---

[1] *See, e.g.*, MGM Studios Inc. v. Grokster, Ltd., 545 U.S. 913 (2005) (applying the doctrine of intentional inducement).

[2] *See* Jonathan Strickland, *How Cloud Storage Works*, HOW STUFF WORKS, http://computer.howstuffworks.com/cloud-computing/cloud-storage.htm (last visited Oct. 25, 2013) (explaining cloud storage).

[3] MEGA HOME PAGE, https://mega.co.nz/ (last visited Mar. 9, 2013).

[4] Lucy Craymer, *Kim Dotcom Launches New Version of Megaupload*, WALL ST. J. (Jan.19, 2013, 1:31 PM), http://online.wsj.com/article/SB10001424127887323968304578251752248253048.html.

[5] Matt Tooley, *Megaupload Gets Shut Down*, SANDVINE: THE BETTER BROADBAND BLOG (Jan. 20, 2012), http://www.betterbroadbandblog.com/2012/01/megaupload-gets-shut-down/.

[6] *Id.*

[7] Indictment, United States v. Kim Dotcom, No. 1:12CR3 (E.D. Va. Jan. 5, 2012), *available at* http://www.washingtonpost.com/wp-srv/business/documents/megaupload_indictment.pdf.

[8] Craymer, *supra* note 4.

[9] MEGA HELP CENTRE, https://mega.co.nz/#help_security (last visited Mar. 9, 2013). See Lee Hutchinson, *Megabad: A quick look at the state of Mega's*

encryption to protect their users' data, MEGA does not store any of the encryption keys on its servers, preventing it from identifying the encrypted information.[10]

An analysis of MEGA's potential liability may provide guidance to other cyberlockers that are evaluating potential liability issues. This Issue Brief proceeds in three Parts. Part I discusses the common-law development of secondary liability doctrine. Part II examines the DMCA's safe harbor for qualifying internet service providers. Finally, Part III considers several key tensions between those safe-harbor provisions and secondary liability, before applying the legal standards to cyberlockers such as MEGA.

I. THE EVOLUTION OF SECONDARY LIABILITY

Copyright law grants six exclusive rights to copyright holders,[11] subject to various limitations.[12] Historically, copyright holders could only enforce their rights against direct infringers.[13] That limitation became problematic when casual copyright infringement, using technology available to consumers, became possible.[14] Rather than pursue the consumers, copyright holders went after the source—the proprietors of the new technologies, against whom an injunction would be far more effective, and, not coincidentally, who had deeper pockets to pay damages. This section will discuss how courts addressed the concerns of rights holders by developing the doctrine of secondary infringement.

A. Sony and the Creation of Contributory Infringement

In *Sony Corp. of America v. Universal City Studios, Inc.*,[15] the Supreme Court held that proprietors of technologies that could be used to infringe copyright could be held secondarily liable for infringement committed by their users.[16] The Court was confronted with Sony's Betamax video tape recorders (VTRs),[17] which gave owners the ability to record

---

encryption, ARS TECHNICA (Jan. 21, 2013 10:22 AM), http://arstechnica.com/business/2013/01/megabad-a-quick-look-at-the-state-of-megas-encryption/, for an explanation and analysis of the encryption schemes employed by MEGA.

[10] MEGA: THE PRIVACY COMPANY, https://mega.co.nz/#privacycompany (last visited Mar. 9, 2013).

[11] 17 U.S.C. § 106 (2012).

[12] *See, e.g.*, §§ 107–112.

[13] *See* JAMES BOYLE, THE PUBLIC DOMAIN 51 (2008) ("In the world of the 1950s . . . [i]t was assumed by many that copyright need not and probably should not regulate private, noncommercial acts.").

[14] *Id.*

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

[16] *See id.* at 435.

[17] *Id.* at 422.

shows on television while being present, away, or watching another show.[18] Universal Studios and Walt Disney Productions, worried about the effect the technology would have on the commercial value of their copyrights, filed suit, seeking both damages and an injunction to prevent Sony from manufacturing and marketing the Betamax.[19]

The crux of the problem was that "[t]he Copyright Act does not expressly render anyone liable for infringement committed by another."[20] Borrowing from patent law's concept of contributory infringement, [21] the Court explained that in order for liability to be imposed on Sony, "it must rest on the fact that they have sold equipment with constructive knowledge of the fact that their customers may use the equipment to make unauthorized copies of copyrighted material."[22] The Court was careful to limit the principle of contributory infringement to instances where the technology is not capable of "commercially significant noninfringing uses."[23] Moreover, the Court did not believe it had to "give precise content to the question of *how much* use is commercially significant."[24]

B. Vicarious Liability and Inducement Liability

In addition to contributory infringement, two other forms of liability exist for potential secondary infringers: vicarious liability and inducement liability. Although the *Sony* Court used the term "vicarious" and "contributory" interchangeably, the doctrine of vicarious liability did not

---

[18] *Id.*

[19] *See id.* at 420–25.

[20] *Id.* at 434. Unlike previous contributory-infringement cases, Sony's "only contact between [itself] and the users of the Betamax . . . occurred at the moment of the sale." *Id.* at 438.

[21] *See id.* at 439 ("There is no precedent in the law of copyright for the imposition of vicarious liability on such a theory. The closest analogy is provided by the patent law cases . . . .")

[22] *Id.* In *Sony*, the Court did not distinguish clearly between contributory and vicarious liability. *See id.*

[23] *See id.* at 442.

[24] *Id.* Both parties had presented "surveys of the way the Betamax" was used, which showed that the "primary using of the machine . . . was 'time-shifting'—the practice of recording a program to view it once at a later time, and thereafter erasing it." *Id.* at 423. Sony's surveys also indicated that "7.3% of all Betamax use is to record sports events, and representatives of professional [sports] testified that they had no objection to the recording of their televised events for home use." *Id.* at 424. This use, among other "private, noncommercial time-shifting" uses was sufficient to meet the Court's standard of "commercially significant noninfringing uses." *See id.* at 442.

arise until much later.[25] In 2005, the Court explained that one may be held liable for vicarious infringement when he "profit[s] from direct infringement while declining to exercise a right to stop or limit it."[26]

In *Metro-Goldwyn*-Mayer *Studios Inc. v. Grokster, Ltd.*, the Supreme Court addressed a new form of liability that can also attach to secondary infringers, including P2P service providers: inducement liability.[27] Once again borrowing from patent-law principles, the Court held that "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."[28] To prevent the newly formed principle from restricting the development of new technologies, the Court was careful to limit its application.[29] First, "mere knowledge of infringing potential or of actual infringing uses" is insufficient to establish liability.[30] Second, "ordinary acts incident to product distribution, such as offering customers technical support or product updates" is similarly insufficient.[31]

C. The DMCA Safe Harbor Provisions

Congress enacted four safe harbors to allow technological proprietors to continue to innovate with immunity from secondary liability as long as they followed certain procedures to limit the infringement taking place on their systems and services.[32] One provision grants qualifying service providers[33] protection for "Information Residing on Systems or Networks at Directions of Users."[34] Specifically, such providers are not liable for copyright infringement "by reason of the storage at the direction of a user of material that resides on a system or network controlled or

---

[25] As the Ninth Circuit explained in *A&M Records, Inc.v. Napster, Inc.*, "[v]icarious copyright liability is an 'outgrowth' of respondeat superior . . . extend[ing] beyond an employer/employee relationship." 229 F.3d 1004, 1022 (9th Cir. 2001) (quoting Fonovisa Inc. v. Cherry Auction, Inc., 76 F.3d 259, 262 (9th Cir. 1996)).
[26] MGM Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 930 (2005).
[27] *Id.* at 936.
[28] *See id.* at 936–37.
[29] *Id.* at 937.
[30] *Id.*
[31] *Id.*
[32] *See* Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 27 (2012).
[33] "Service providers" under the statute are more than just those who provide internet service; they are any "entit[ies] offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received." 17 U.S.C. § 512(k)(1) (2012).
[34] § 512(c).

operated by or for the service provider."[35] However, the safe harbor only applies if the 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;
>
> (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 as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.36

Additionally, the DMCA requires service providers to implement a repeat-infringer policy.[37] Finally, DMCA safe harbors do not require service providers to "monitor[] [their] service[s] or affirmatively seek[] facts indicating infringing activity, except to the extent consistent with" the service's repeat-infringer policy.[38]

II. ADDRESSING ISSUES WITHIN THE DMCA

Two important issues that remain unclear are whether the DMCA safe harbor applies in cases of inducement liability[39] and whether the actual and "red flag" knowledge provisions require indication of "specific and identifiable infringements."[40]

---

[35] § 512(c)(1).
[36] §§ 512(c)(1)(A)–(C).
[37] § 512(i)(1)(A) (requiring 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").
[38] *See* § 512(m)(1).
[39] *See generally* R. Anthony Reese, *The Relationship Between the ISP Safe Harbors and Liability for Inducement*, 2011 STAN. TECH. L. REV. 8. The safe harbor was implemented before the Supreme Court created inducement liability in *Grokster*.
[40] Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 30 (2d Cir. 2012) (quotation marks omitted). "Red flag" knowledge refers to § 512(c)(1)(A)(ii).

A. The DMCA's Application to Inducement Liability

Various theories have been presented suggesting that inducement liability precludes application of the DMCA safe harbors.[41] First, Congress did not anticipate the DMCA's application to inducement liability because the DMCA was enacted before the *Grokster* opinion created such liability.[42] Second, the DMCA "safe harbors are based on passive good faith conduct at operating a legitimate Internet business" while inducement liability is based on "active bad faith conduct promoting infringement."[43] However, these two ideas cannot be reconciled with the history and application of the DMCA. This section evaluates these positions and discusses how inducement liability may coexist with the DMCA safe harbors even though these two arguments fail.

Contrary to the first argument, the safe harbors were created to withstand the development of other, additional secondary liability schemes.[44] Congress anticipated that the law of copyright would evolve and chose to create a series of safe harbors rather than codify existing standards of secondary liability.[45] Furthermore, the safe harbors explicitly state that "service provider[s] shall not be liable . . . for infringement of copyright" without predicating such protection on a particular type of infringement.[46] Although some courts have considered the DMCA a restatement of existing forms of liability,[47] others have found that such a reading would limit Congress' purpose in establishing safe harbors as an evolving tool.[48]

With respect to the second argument, it is at least plausible that a finding of inducement infringement would not preclude safe harbor under the DMCA. Although inducement often looks to a service provider's actions in promoting infringement and the DMCA requires good-faith, passive conduct in determining protection, inducement may not "necessarily

---

[41] *See generally* Columbia Pictures Indus., Inc. v. Fung, No. CV 06-5578, 2009 U.S. Dist. LEXIS 122661 (C.D. Cal. Dec. 21, 2009).
[42] *See* Daniel Kohler, *A Question of Intent: Why Inducement Liability Should Preclude Protection Under the Safe Harbor Provisions of the Digital Millennium Copyright Act*, 41 SW. L. REV. 487, 490 (2012).
[43] *Fung*, 2009 U.S. Dist. LEXIS 122661, at *67–68.
[44] *See YouTube*, 676 F.3d at 27.
[45] *See id.*
[46] 17 U.S.C. § 512(a) (2012).
[47] *See Fung*, 2009 U.S. Dist. LEXIS 122661, at *57 ("In many ways, the Digital Millennium Copyright Act is simply a restatement of the legal standards establishing secondary copyright infringement . . . .").
[48] *YouTube*, 676 F.3d at 27.

be limited to . . . active, bad-faith conduct."[49] For example, under one particular reading of *Grokster*, it is feasible that *any* online service provider whose service is capable of infringement may be liable for inducement.[50] A categorical exclusion of DMCA protection would, therefore, impose liability on service providers in instances where Congress sought to protect technological innovators.[51] Instead, the DMCA's protections can be limited to service providers that do not possess "red flag" knowledge of infringement.[52] The ISP safe harbor's "red flag" knowledge provision would preclude protection for "service provider[s] who actively encourage[] users to infringe [because they] will likely at least be 'aware of facts or circumstances from which infringing activity is apparent.'"[53]

B. The Appropriate Standard of Knowledge

The ISP safe-harbor provision's requisite standard of knowledge poses an additional problem to be resolved. The ISP safe harbor applies unless the service provider has "actual knowledge" or is "aware of facts or circumstances" of infringing activity.[54] Additionally, service providers must "upon obtaining such knowledge or awareness, act expeditiously to remove . . . the material."[55] As the *YouTube* court correctly pointed out, "the nature of the removal obligation itself contemplates knowledge or awareness of *specific* infringing material, because expeditious removal is possible only if the service provider knows with particularity which items to remove."[56] With respect to the "actual knowledge" requirement, a specificity standard is clear, but whether such a specificity standard can be applied to the "red flag" requirement poses a dilemma. Arguably, the "red flag" provision of the ISP safe harbor would become superfluous with the specificity

---

[49] *See, e.g.*, Reese, *supra* note 39, at 16–17 (arguing service providers that have "substantial certainty" of infringing activity on their services may be found to be contributorily liable).

[50] *See id.* at 17 ("After all, *some* of the provider's users are almost certain to store infringing material, at least if the provider's service attracts any substantial number of users.").

[51] *See* H.R. REP. NO. 105-551, pt. 2, at 23 (1998) ("The Committee . . . believes it is important . . . to understand the practical implications of th[e] relationship [between intellectual property and electronic commerce] on the development of technology to be used in promoting electronic commerce.").

[52] *See id.* at 24.

[53] *Id.* (quoting 17 U.S.C. § 512(c)(1)(A)(ii) (2006)).

[54] 17 U.S.C. §§ 512(c)(1)(A)(i)–(ii).

[55] § 512(c)(1)(A)(iii).

[56] *YouTube*, 676 F.3d at 30.

requirement because knowledge or awareness of specific infringing material would also establish the "actual knowledge" provision.[57]

The *YouTube* court held that the difference between the "actual knowledge" and "red flag" requirements was between a subjective and objective belief, respectively.[58] Because the "red flag" provision "incorporates an objective standard," it was distinguished from the actual knowledge provision such that both could "do independent work and both [could] apply only to specific instances of infringement."[59] The Ninth Circuit in *UMG Recordings v. Shelter Capital Partners*, on the other hand, agreed that a specificity requirement existed with respect to infringing material, but found no distinction between its application to the "actual knowledge" and "red flag" requirements.[60] Instead, that court held that "the burden remains with the copyright holder rather [than] the service provider" to show specific infringing material because service providers do not have a duty to actively search for such material.[61]

The Ninth Circuit's reluctance to distinguish between the "actual knowledge" and "red flag" requirements with respect to a finding of specific infringing material was largely due to its reluctance to impose any duty to monitor for infringing material.[62] Such a duty, it said, would run afoul of the safe harbor provisions.[63] However, in so doing, the Ninth Circuit rendered both provisions substantially similar, if not identical.[64] The *YouTube* court's construction avoids such a problem. Moreover, it allows for liability in situations when the service provider is subjectively unaware of specific infringement but aware of facts that would otherwise indicate such a finding to a reasonable person.[65] Providing such a flexible standard protects the rights of copyright holders while balancing the interests of and protections granted to technology proprietors.

---

[57] *See id.* at 31.
[58] *See id.* The court explained, "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." *Id.*
[59] *Id.*
[60] 667 F.3d 1022, 1037–38 (9th Cir. 2011).
[61] *See id.* at 1038.
[62] *See id.*
[63] *See id.* at 1041; *see also* 17 U.S.C. § 512(m) (2012).
[64] The *YouTube* court was worried precisely about this: rendering the "red flag" provision superfluous.
[65] Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 31 (2d Cir. 2012).

C. Does MEGA Evade Liability?

The determination of copyright liability—direct and secondary—is largely contextually driven and an *ex ante* analysis of potential liability for a new technology may only provide limited guidance. Without the benefit of discovery, evidence that would establish liability or support protection under the DMCA remains in the sole province of the technological proprietor. This section will address whether MEGA's cyberlocker implementation of various methods might foreclose protection under the DMCA.[66]

MEGA's use of user-controlled encryption is unique among cyberlockers. MEGA boasts that using UCE will provide greater security and protection for users of its service over other cyberlockers. However, because MEGA's predecessor was largely infamous (and ultimately shut down) for copyright infringement, courts may view UCE as evidence of an attempt to circumvent the requisite knowledge or awareness under the DMCA ISP safe harbor. At least one court has addressed the use of encryption technology in a P2P service. In *In re Aimster Copyright Litigation*,[67] the Seventh Circuit held that the use of encryption technology in a P2P music-sharing service could not shield the creator from knowledge.[68] Instead, the court found that the use of encryption amounts to willful blindness, which would be sufficient to meet the knowledge requirement for contributory infringement.[69] In *YouTube*, the Second Circuit noted that although the DMCA does not "'speak directly' to the willful blindness doctrine, . . . [it] may be applied, in appropriate circumstances, to demonstrate knowledge or awareness of specific instances of infringement under the DMCA."[70] It is likely that other courts would subscribe to this analysis because the doctrine of "willful blindness . . . is hardly [a] novel" concept and would prevent an infringer from "shield[ing] itself from

---

[66] Whether cyberlockers can be exempt from liability under fair use, 17 U.S.C. § 107 (2012), is outside the scope of this Issue Brief.

[67] In re Aimster Copyright Litigation, 334 F.3d 643 (7th Cir. 2003).

[68] *Id.* at 650–51.

[69] *See id.* ("Our point is only that a service provider that would otherwise be a contributory infringer does not obtain immunity by using encryption to shield itself from actual knowledge of the unlawful purposes for which the service is being used."); *see also YouTube*, 676 F.3d at 35 ("A person is 'willfully blind' or engages in 'conscious avoidance amounting to knowledge where the person 'was aware of a high probability of the fact in dispute and consciously avoided that fact.'" (quoting United States v. Aina-Marshall, 336 F.3d 167, 170 (2d Cir. 2003) (internal quotation marks omitted)).

[70] *YouTube*, 676 F.3d at 34–35 (quoting Matar v. Dichter, 563 F.3d 9, 14 (2d Cir. 2009)).

learning of the particular infringing transactions by looking the other way."[71]

If evidence suggests that MEGA implemented UCE for more than just security, but rather to evade knowledge of infringing activity, the provider may be found to be willfully blind, thereby imputing the requisite level of knowledge that would require removal of the infringing material under the DMCA. Such a finding may even be supported by MEGA's use of deduplication.[72] Although deduplication may be used for efficiency gains,[73] the use of UCE coupled with deduplication means that each file uploaded onto the service provider may be viewed as its own stand-alone file. For copyright holders, this presents a vexing problem: Each piece of copyrighted material that gets uploaded to the service would require a separate takedown notice. Because service providers have no duty to monitor their service and the application of UCE greatly restricts a service provider's ability to do so, copyright holders would face an uphill battle against third party infringers using the service. Again, such a scheme may support a finding that MEGA possesses the requisite "red flag" knowledge under the DMCA.[74]

Another unique issue with respect to MEGA's service is its use of distributed host servers.[75] Whether MEGA "receive[s] a financial benefit *directly* attributable to the infringing activity" can only be determined through the course of litigation.[76] Often, a service provider's business model will help establish whether there is a direct link between the financial benefit and the infringing activity.[77] Like many other cyberlockers, MEGA offers both free and premium services. The premium services, which

---

[71] *See id.* at 35 (quoting Tiffany (NJ) Inc. v. eBay, Inc., 600 F.3d 93, 109 (2d Cir. 2009)).

[72] Deduplication is a process of removing duplicated data on a server. For example, if two users update the identical file, one may be deleted and the user of that file will be given a reference to the original. *See* Rick Vanover, *Storage-based compression and deduplication overview*, TECHREPUBLIC (Nov. 13, 2009, 1:41 PM), http://www.techrepublic.com/blog/datacenter/storage-based-compression-and-de-duplication-overview (explaining data deduplication).

[73] For example, the removal of duplicated data saves decreases server storage space. *Id.*

[74] *See* 17 U.S.C. § 512(c)(1)(A)(ii) (2012).

[75] MEGA allows host partners to provide servers to support its service. MEGA HOSTING PARTNERS, https://mega.co.nz/#hosting (last visited Apr. 6, 2013).

[76] *See* § 512(c)(1)(B) (emphasis added).

[77] *See, e.g.*, Reese, *supra* note 39, at 20 ("[T]he Court viewed the defendants' business model as a 'complement' to direct evidence in the record of unlawful intent to encourage infringement . . . ."); Jacqueline C. Charlesworth, *The Moral of the Story: What* Grokster *Has to Teach About the DMCA*, 2011 STAN. TECH. L. REV. 6.

charges users a fee based on data storage, does not immediately trigger suspicion that there is a link between the financial benefit and the infringing material. More troubling is MEGA's use of distributed host servers. Although it possesses its own servers, MEGA allows third parties to act as servers for storage of content.[78] MEGA claims this ensures that data stored on its service will be available even if one or more of its servers goes down.[79] It is unclear what level of control MEGA maintains over these host servers; presumably it is able to exert some form of control over host servers if it is able to comply with takedown notices. Even so, as the *YouTube* court made clear, the "right and ability to control" must be "something more" than traditional vicarious liability.[80] Here, the court's inclusion of inducement as evidence of such control would be particularly telling. Specifically, courts may find that MEGA's use of UCE, deduplication, and distributed host servers were all "affirmative steps taken to foster infringement."[81]

CONCLUSION

Even if MEGA does not qualify for DMCA protection, courts would be prudent to limit their holding to MEGA's service (and others like it). An overbroad application may hamper the development of new technologies, including next-generation cyberlockers—a goal that runs afoul of Congress' purpose in establishing the DMCA.[82] Although many of the mechanisms MEGA employs may exist in a gray area between protection and infringement, they are not entirely unique to MEGA. Cyberlockers all maintain their own standards for addressing infringement, deduplication, encryption, and file hosting. MEGA's decision to employ certain schemes should not be considered to violate the DMCA requirements solely because of its predecessor site's bad media image, but instead, because there is a direct showing that the current service was developed and employed in a manner that violates the DMCA and secondary-infringement principles.

---

[78] Chris Keall, *Building Mega: Ars' pre-launch interview with Kim Dotcom*, ARS TECHNICA (Jan 19, 2013, 12:10 AM), http://arstechnica.com/tech-policy/2013/01/building-mega-ars-pre-launch-interview-with-kim-dotcom/.
[79] *Id.*
[80] *See* Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 38 (2d Cir. 2012).
[81] Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 45 U.S. 913, 937 (2005).
[82] *See* H.R. REP. NO. 105-551, pt. 2, at 23 (1998) ("The Committee . . . believes it is important . . . to understand the practical implications of th[e] relationship [between intellectual property and electronic commerce] on the development of technology to be used in promoting electronic commerce.").