A HYPOTHETICAL NON-INFRINGING NETWORK: AN EXAMINATION OF THE EFFICACY OF SAFE HARBOR IN SECTION 512(C) OF THE DMCA

CASSIUS SIMS[1]

ABSTRACT

This iBrief will present a hypothetical network that allows dissidents to transfer information outside the watchful eye of an oppressive government. It will argue that because a network operator meets the requirements of the safe harbor of section 512(c) of the Digital Millennium Copyright Act, the hosts of the network are immune from any vicarious copyright liability.

INTRODUCTION

¶1 Suppose you believe in supporting nascent democracies. While trawling the web, you come across a software client, promoted as a way to help dissidents in oppressed regimes. All you have to do is download the client and let your computer help the movement. Would you participate?

¶2 Consider a network designed to support democracy activists. To conceal the activists' identities and plans, software developers design the network to prevent any user from knowing where data has come from, where it is going, and what the data represents. Indeed, the network would allow activists of all stripes to trade documents outside the snooping power of oppressive governments. Individual users—like you—are only asked to provide some hard drive space and an Internet connection. The network transfers data through several different users, providing more secrecy and reliability. You, however, will not know from whom the data comes, or the content stored on your computer.

¶3 This secrecy may encourage illegal file sharers to use your computer indirectly to transfer illegal files. Are you liable for their illegal activities? Should you be liable? This iBrief will argue that, because of the way this network has been constructed, the language of section 512 of the Digital Millennium Copyright Act (DMCA) allows people like you to use a safe harbor from copyright infringement.

---

[1] Cassius Sims is a J.D. Candidate at Duke University School of Law, class of 2010. He would like to thank his family for their support through undergraduate and law school, his advisor Professor Jennifer Jenkins for her many helpful suggestions, and Sam Slee for his help discussing the network.

¶4 The Digital Millennium Copyright Act of 1998 updated the Copyright Act to reflect a digital world.[2] Congress hoped to provide "greater certainty to service providers concerning their legal exposure for infringement that may occur in the course of their activities."[3] This iBrief will explore the applicability of safe harbors codified in 17 U.S.C. § 512 to a hypothetical network. By designing a network to allow free transfer of data, such a network would also provide a way for users to distribute data that may infringe copyright. As this note will argue, entities storing potentially infringing material may moor in the safe harbor of section 512(c) of the DMCA.

¶5 First, the note will discuss the components of section 512. Second, it will describe a hypothetical network. Third, it will apply section 512(c) to the hypothetical network. Finally, the note will consider the legality of the network in light of other bodies of law.

I. THE SECTION 512 SAFE HARBORS

¶6 The DMCA provides a safe harbor from liability for copyright infringement for four types of services that an entity may provide its users: transitory digital network communications,[4] system caching,[5] information residing on systems or networks at the direction of users,[6] and information location tools.[7]

¶7 Section 512(a) applies to large Internet Service Providers (ISPs).[8] Congress intended that this section provide a safe harbor to companies like Verizon and AT&T.[9] The statute allows service providers that transmit, route, or provide connections to disclaim liability from secondary copyright infringement.[10] As a part of a connection between users, potentially infringing material may be copied as data is transferred.[11] For this safe harbor to apply, any copies made must be of a

---

[2] Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (codified in scattered sections of 17 U.S.C.).
[3] S. REP. NO. 105-190, at 20 (1998) [hereinafter *Senate Report*].
[4] 17 U.S.C. § 512(a) (2007).
[5] § 512(b).
[6] § 512(c).
[7] § 512(d).
[8] *See* § 512(a).
[9] *Senate Report*, *supra* note 3, at 41 ("Section (a) applies to communications functions associated with sending digital communications of others across digital networks, such as the Internet and other online networks.").
[10] § 512(a).
[11] *Senate Report*, *supra* note 3, at 41 ("Section (a) applies to service providers transmitting, routing, or providing connections for material, and some forms of

transient nature.[12] Without section 512(a), the Internet would not likely exist as it does today.

¶8 Section 512(b) protects companies that cache data while providing connections to customers.[13] Caching speeds up access to content accessed by more than one user.[14] It requires copying the data returned by a user's request for data from a remote server.[15] While caching, the service provider may infringe copyright because the service provider reproduces copyrighted material. This copy, however, simply allows the local server to provide data to a subsequent user without transferring duplicate data over the Internet. Section 512(b) codifies the legality of this practice, which increases the efficiency of the Internet.

¶9 The third provision, section 512(c), protects companies from liability arising from material posted by a user.[16] Specifically, the DMCA provides a safe harbor from most monetary and injunctive relief when a service provider would otherwise be liable for an "infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider."[17] Auction[18] and shopping[19] websites have safely moored in this safe harbor. An operator of the hypothetical network developed in this iBrief will attempt to use the safe harbor provided for "storage at the direction of a user."

¶10 Finally, section 512(d) protects companies that index, refer to, and link to websites that infringe copyright.[20] Search engines commonly index content without verifying the legality of linked content. When

---

intermediate and transient storage of material in the course of performing these functions.").

[12] *Id*.

[13] § 512(b).

[14] *Senate Report*, *supra* note 3, at 41 ("In terminology describing current technology, this storage is a form of "caching," which is used on some networks to increase network performance and to reduce network congestion generally, as well as to reduce congestion and delays to popular sites.").

[15] *See id*. at 42 ("The material in question is stored on the service provider's system or network for some period of time to facilitate access by users subsequent to the one who previously sought access to it.").

[16] *Id*. at 43 ("Examples of such storage [applicable in section (c)] include providing server space for a user's web site, for a chatroom, or other forum in which material may be posted at the direction of users.").

[17] § 512(c).

[18] *See, e.g.*, Hendrickson v. eBay, Inc., 165 F.Supp. 2d 1082 (C.D. Cal. 2001).

[19] *See, e.g.*, Corbis Corp. v. Amazon.com, Inc., 351 F.Supp. 2d 1090 (W.D. Wash. 2004).

[20] § 512(d).

enacting the DMCA, Congress recognized the importance of indexing the Internet through search engines.[21]

¶11 This iBrief will focus on the applicability of section 512(c) to a hypothetical network. Section 512(c) allows a service provider to disclaim liability from copyright infringement arising from information stored on its systems at the direction of a user.[22] Before discussing section 512(c) and its related provisions in detail, the iBrief will present the hypothetical network.

II. THE HYPOTHETICAL NETWORK

¶12 This iBrief will first discuss the components of the network and then discuss the connection between components. There are several components to the hypothetical network. This iBrief will assume an initial user, three intermediate users, and a final user exist. The initial user (U0) transfers a file to intermediate users, who store the files and consequently transfer the file to the final user (UF). Each user that connects to an intermediate user for the first time must agree to policies mandated by the intermediate user.

¶13 The network extends normal peer-to-peer file sharing technology. Additionally, the hypothetical network uses two programs to maintain the secrecy of the identity and content of the files. The first program encrypts the file so it is not easily comprehensible without decryption using an encryption key. The second program, using an encoding key, the size of the original file, and the original filename, splits the encrypted file into pieces and generates filenames for each piece. UF uses these programs in reverse order to recreate the original file. UF and U0 pass the two keys (encryption and encoding) off-network. Put another way, UF and U0 transfer the keys over another network, such as by telephone. Therefore, only U0 and UF can combine and decrypt the file pieces to recreate the original file. Modern cryptography techniques can be applied to a real network based on this hypothetical network. For example, a public/private key system could be used in this network.

¶14 In the hypothetical network, before U0 uploads a file to the service providers, U0 runs the two programs. Once U0 has encrypted and split the original file, U0 broadcasts a request for storage to the

---

[21] *Senate Report*, *supra* note 3, at 49 ("This provision is intended to promote the development of information location tools generally, and Internet directories such as Yahoo!'s in particular, by establishing a safe-harbor from copyright infringement liability for information location tool providers if they comply with the notice and takedown procedures and other requirements of section (d).").

[22] § 512(c).

intermediate users. Any intermediate user that will accept storage responds affirmatively. U0 transfers each file piece to a different intermediate user. When UF wants to find a file, UF enters the original file size, encoding key and original filename into the second application to generate the names of the files that constitute the original file. UF then searches for the file pieces on the network following standard peer-to-peer network techniques. Once UF downloads all of the file pieces, UF can recreate the original file with the encryption key and first program.

¶15 The hypothetical network explained above intentionally abstracts the network for clarity. Moreover, although it may seem complex, this hypothetical network could be implemented rather easily with software.[23] This iBrief will not discuss the liability of U0 and UF or the software developer. First, if U0 and UF infringe copyright, the safe harbors of section 512 are inapposite to their liability. Moreover, illegal file sharers are not the intended users of the network. Second, potential liability for software developers involves unresolved legal questions beyond the purview of this iBrief. The iBrief will argue that the intermediate users that host files may disclaim liability for copyright infringement under section 512(c) of the DMCA.

III. DISSECTING SECTION 512(C) OF THE DMCA

¶16 An entity must pass through several locks before mooring in the safe harbor provided by section 512. Section 512(c) provides that:

> A service provider shall not be liable for monetary relief, or, except as provided in section (j), for injunctive or other equitable relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, 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;

[23] An existing network that would likely fit within this hypothetical network is Freenet. *See* The Freenet Project, http://freenetproject.org (last visited Oct. 31, 2009).

> (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.[24]

¶17 To apply this statute to the hypothetical network, this iBrief will first discuss the threshold requirements for entities wishing to utilize the safe harbors of section 512. It will then discuss the statutory requirements of section 512(c). For each requirement, this iBrief will discuss the current state of the law and then apply the law to the network as described.

A. The Definition of a Service Provider

¶18 Section 512(k)(1)(B) defines service provider as: "a provider of online services or network access, or the operator of facilities therefor."[25] Some plaintiffs have argued that entities must provide data connections, like an internet service provider, to qualify for service provider status.[26] Courts, however, have construed the definition of service provider broadly, including websites in the definition.[27] Although courts have interpreted the definition of service provider broadly to include many types of services, courts have not determined if an entity must meet a minimum size requirement to qualify as a service provider.

¶19 Courts have allowed many entities to claim service provider status. In *Corbis Corp. v. Amazon.com, Inc.*, the Western District of Washington held that Amazon was a service provider when it provided website space to third party sellers.[28] Corbis alleged that several of Amazon's third party sellers infringed copyrights held by Corbis.[29] The

---

[24] § 512(c).
[25] § 512(k)(1)(B).
[26] *See* Corbis Corp. v. Amazon.com, Inc., 351 F.Supp. 2d 1090, 1100 n.6 (W.D. Wash. 2004) ("Corbis argues that Amazon is not a service provider because Amazon does not serve to route or connect online digital communications.' This argument is unavailing. The relevant definition of service provider does not require Amazon to engage in such activity." (citations omitted)).
[27] *Id.*
[28] *Id.* at 1100 ("Amazon operates web sites, provides retail and third party selling services to Internet users, and maintains computers to govern access to its web sites. These activities fall squarely within the broad scope of the § 512(k)(1)(B) definition of 'service provider'." (footnotes omitted)).
[29] *Id.* at 1097 ("Corbis has identified a total of 232 images . . . in which it claims a copyright interest. Two of the images appeared on the IMDb website. The

court wrote that Amazon's selling and serving customers falls "squarely within the broad scope of the § 512(k)(1)(B) definition of 'service provider' . . . ."[30] Extending to providers beyond the World Wide Web, *In re Aimster Copyright Litigation* held that: "[a]lthough the Act was not passed with Napster-type services in mind, the definition of Internet service provider is broad, . . . and, . . . Aimster [a Napster type service] fits it."[31] Although the *In re Aimster* court rejected Aimster's attempt to pursue the safe harbor of section 512, the court concluded that distribution networks were considered service providers under section 512(k)(1)(B).[32] Since the courts have interpreted this provision broadly, an internet storage provider should fall within the definition of service provider of section 512(c).

¶20 Although the case law allows many services to qualify as service providers, the case law does not clearly state what size entities must be to qualify as service providers. Large companies like Amazon[33] and eBay[34] have easily passed the bar as service providers. In *ALS Scan, Inc. v. RemarQ Communities, Inc.*,[35] a unanimous panel of the Fourth Circuit held that even smaller entities were service providers.[36] Remarq was, in Internet terms, a small provider. At the time of litigation, it provided access to 24,000 subscribers,[37] and "remove[d] [user-posted materials] after about 8–10 days to accommodate its limited server capacity."[38] Both parties conceded that size did not disqualify Remarq from service provider status.[39] Size has not been litigated as a matter of practicality: since section 512(c) requires that service providers lack knowledge of

---

remaining 230 images have been copied, displayed, and sold by vendor defendants through their zShops sites.").

[30] *Id.* at 1100.

[31] 334 F.3d 643, 655 (7th Cir. 2003).

[32] *Id.* ("Aimster fits [the definition of a section 512 service provider].").

[33] *Corbis*, 351 F.Supp. 2d at 1100 ("Amazon operates web sites, provides retail and third party selling services to Internet users, and maintains computers to govern access to its web sites. These activities fall squarely within the broad scope of the § 512(k)(1)(B) definition of 'service provider'." (footnotes omitted)).

[34] Hendrickson v. eBay, Inc., 165 F.Supp. 2d 1082, 1088 (C.D. Cal. 2001) ("There is no dispute over whether eBay is an Internet 'service provider' within the meaning of Section 512.").

[35] 239 F.3d 619 (4th Cir. 2001).

[36] *Id.* at 623 ("Neither party to this case suggests that RemarQ is not an Internet service provider for purposes of the Act.").

[37] *Id.* at 620 ("[RemarQ] has approximately 24,000 subscribers.").

[38] *Id.*

[39] *Id.* at 623.

infringement,[40] most small service providers would be denied the safe harbor because they would be aware of the legality or illegality of activity occurring on their networks. This iBrief asserts that a single user qualifies as a service provider as defined by section 512(k)(1)(B). This assertion is based on the broad language in section 512. In further defining service provider, the section states that a service provider is an entity that provides "online communications, between or among points specified by a user, of material of the user's choosing."[41] The legislative history neither promotes nor prohibits this characterization; the Senate Report simply states that the category is intentionally broad.[42]

¶21 In the hypothetical network, the intermediate users can properly claim service provider status under the definition of a service provider in section 512(k)(1)(B). The intermediate users provide "online communications, between or among points specified by a user, of material of the user's choosing . . . ."[43] The intermediate users provide online communications between U0 and UF. U0 chooses the material. Therefore, the intermediate users pass the first hurdle in claiming protection from liability for the information that they store. For the remainder of the iBrief, the intermediate users will be called service providers.

B. A Termination Policy

¶22 Section 512(i)(1)(A) requires that a service provider "has adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, 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."[44] The Senate Report stated that Congress wanted users who "abuse their access to the Internet through disrespect for the intellectual property rights of others [to] know that there is a realistic threat of losing that access."[45] A user termination policy fits this requirement. There are two independent requirements: adoption of a policy and its reasonable implementation.

---

[40] *See infra* Part III.E.
[41] 17 U.S.C. § 512(k)(1)(A) (2007).
[42] *Senate Report*, *supra* note 3, at 54–55 (1998) (stating that the service provider definition for section (b)–(d) is broader than that for section (a), but not giving a better explanation of the definition).
[43] § 512(k)(1)(A).
[44] § 512(i)(1)(A).
[45] *Senate Report*, *supra* note 3, at 52.

¶23 First, section 512(i)(1)(A) requires that service providers inform users of the consequences of using a network for copyright infringement.[46] The language of the statute, however, allows the provider latitude in designing the policy.[47] In *Corbis*, Amazon required that sellers agree to a user termination policy before selling on Amazon.[48] Although Amazon's policy did not "precisely track the language of the DMCA," the court held that the policy was properly constructed.[49] The Western District of Washington noted that the policy prohibited the "listing, linking, or posting of any material that violates copyright laws," and warned infringers that Amazon may penalize users by "restricting access to Amazon's sites and suspen[ding] or terminat[ing users'] service."[50] A policy that states the crime and potential liability should pass muster under the DMCA. Furthermore, the statute does not require that service providers demonstrate user policy enforcement.[51] Therefore, even if the provider has not actually terminated users, the provider should be protected by the safe harbor if it has a policy consistent with the requirements of section 512.[52]

¶24 Reasonable implementation of a user policy "permits service providers to implement a variety of procedures, but an implementation is reasonable if, under 'appropriate circumstances,' the service provider terminates users who repeatedly or blatantly infringe copyright."[53] The service provider legally cannot actively promote infringement;[54] a policy

---

[46] Ellison v. Robertson, 357 F.3d 1072, 1080 (9th Cir. 2004) ("Section 512(i)(1)(A) requires service providers to . . . inform its subscribers of the policy.").

[47] Corbis Corp. v. Amazon.com, Inc., 351 F.Supp. 2d 1090, 1101 (W.D. Wash. 2004) ("This open-ended language contrasts markedly with the specific requirements for infringement notices and take-down procedures set forth in § 512(c).").

[48] *Id.* ("Each vendor must agree to the terms of the Participation Agreement before selling on the [Amazon website].").

[49] *Id.*

[50] *Id.*

[51] Todd E. Reese, Comment, *Wading through the Muddy Waters: The Courts' Misapplication of Section 512(c) of the Digital Millennium Copyright Act*, 34 SW. U. L. REV. 287, 298 (2004) ("Nowhere does the statute say that the policy must have been applied to a specific individual. Thus, an [online service provider] must simply make a good faith effort at consistently applying its policy.").

[52] *See id.* (noting that a policy does not necessarily need to be enforced to qualify under the safe harbor).

[53] Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1109 (9th Cir. 2007).

[54] *See In re* Aimster Copyright Litig., 334 F.3d 643, 655 (7th Cir. 2003) (determining that active promotion of infringement does not allow a company to

to prohibit infringement must be combined with actual termination of users.[55] In *CCBill*, the Ninth Circuit held that "a service provider 'implements' a policy 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."[56] Moreover, the Ninth Circuit held that section 512(c) does not require that a service provider monitor the material or activity on its network.[57] In *Corbis Corp. v. Amazon.com, Inc.*, Corbis noted "Amazon's infringement policy has not been able to prevent certain vendors from reappearing on the zShops platform under pseudonyms."[58] Corbis then asserted "that Posternow's reappearance shows that the infringement policy is a failure."[59] Disagreeing, the court held that the DMCA does not require impeccable implementation of the user policy: "The mere fact that [a user] appeared on [the service] under a different user name and identity does not, by itself, create a legitimate question of fact regarding the procedural implementation of Amazon's termination policy."[60] Similarly, in *Io Group, Inc. v. Veoh Networks, Inc.*, the Northern District of California suggested that a website consisting of user-posted videos had reasonably implemented their user policy.[61] In *Io Group*, the plaintiff argued that Veoh's policy was not reasonably implemented because it was easy to obtain an email address, and an email address was all that was required to subscribe to the service.[62] The court rejected this argument and held for the defendant.[63] These holdings demonstrate that the safe harbor in section 512(c) is not predicated on a proactive search for infringing material.

---

use the safe harbor, the court wrote that "[f]ar from doing anything to discourage repeat infringers of the plaintiffs' copyrights, Aimster invited them to do so . . . .").

[55] *See id.* ("The common element of its safe harbors is that the service provider must do what it can reasonably be asked to do to prevent the use of its service by 'repeat infringers.'").

[56] 488 F.3d at 1109.

[57] *See id.* at 1111 ("To identify and terminate repeat infringers, a service provider need not affirmatively police its users for evidence of repeat infringement.").

[58] 351 F. Supp. 2d 1090, 1103 (W.D. Wash. 2004).

[59] *Id.*

[60] *Id.* at 1104.

[61] 586 F. Supp. 2d 1132, 1145 (N.D. Cal. 2008).

[62] *Id.* at 1143–44.

[63] *Id*. at 1144 (holding that simply because the plaintiff was able to make two suspiciously named email accounts and sign up independently under each does not amount to lack of a repeat infringer policy).

¶25 A service provider must have a policy, inform its users of the policy, and reasonably implement the policy.[64] In the hypothetical network, each service provider has a policy and informs users of the policy during a user's first connection.[65] If constructed properly, the agreement will satisfy the user policy requirement. Since a provider must know that a user is infringing copyright to implement the user policy, reasonable implementation will not be required until the service provider obtains knowledge of infringement. Each service provider has no idea whatsoever what data it is holding for the network.[66] Moreover, a service provider will never receive an infringement notice and therefore never become aware of infringement.[67] Service providers comply with section 512(i)(1)(A) as long as its user policy describes consequences for copyright infringement, the service provider informs users of the policy, and, in the unlikely event that the service provider receives repeat notifications of infringement, the service provider terminates the user. Since the hypothetical network satisfies all of these criteria, the service providers should qualify for the section 512(c) safe harbor.

C. Accommodation of Standard Technical Measures

¶26 Section 512(i)(1) of the DMCA requires that providers accommodate standard technical measures: "The limitations on liability established by this section shall apply to a service provider only if the service provider . . . accommodates and does not interfere with standard technical measures."[68] Section 512(i) then defines "standard technical measures."

> [T]echnical measures that are used by copyright owners to identify or protect copyrighted works and—
>
> (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

---

[64] Ellison v. Robertson, 357 F.3d 1072, 1080 (9th Cir. 2004) ("Section 512(i)(1)(A) requires service providers to: (1) adopt a policy that provides for the termination of service access for repeat copyright infringers in appropriate circumstances; (2) implement that policy in a reasonable manner; and (3) inform its subscribers of the policy.").
[65] *See supra* Part II.
[66] *See supra* Part II.
[67] *See infra* Part III.H
[68] 17 U.S.C. § 512(i)(1) (2007).

> (C) do not impose substantial costs on service providers or substantial burdens on their systems or networks.[69]

¶27 Rarely do plaintiffs allege that service providers interfere with standard technical measures.[70] Even when presented with a question of what constituted standard technical measures, the Ninth Circuit was "unable to determine . . . whether accessing websites is a standard technical measure."[71] The Central District of California has held that "[i]t thus appears to be an open question if *any* conduct or policy could interfere with 'standard technical measures.'"[72] In *Corbis*, using a website was the way in which rights holders found infringing material.[73] If there is no cognizable standard technical measure, no court could hold that a service provider violated this requirement for safe harbor.

¶28 In the hypothetical network, the system design may frustrate attempts to access the material. The service providers do not frustrate access—the programs used before placing files on the network frustrate access. Since there does not seem to be a cognizable "standard technical measure" and the service providers do nothing to interfere with a rights holder's ability to search for infringing content on the network, the service providers in the hypothetical network comply with section 512(i).

D. Storage at the Direction of the User

¶29 The safe harbor in section 512(c) shields service providers from liability arising from infringing material stored at the direction of the user.[74] In some cases, courts and parties have simply assumed that

---

[69] 17 U.S.C. § 512(i)(2).

[70] *See, e.g.*, Io Group, Inc. v. Veoh, Inc., 586 F. Supp. 2d 1132, 1143 (N.D. Cal. 2008) ("Nor does [Io] dispute that Veoh . . . accommodates, and does not interfere with, 'standard technical measures' used to protect copyrighted works."); Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, 1106 (W.D. Wash. 2004) ("Corbis has not challenged Amazon's assertion that it accommodates and does not interfere with standard technical measures used to identify and protect copyrighted works.").

[71] Perfect 10 Inc. v. CCBill LLC, 488 F.3d 1102, 1115 (9th Cir. 2007).

[72] Perfect 10 Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1174 n.18 (C.D. Cal. 2002).

[73] *See* 351 F. Supp. 2d at 1097 ("Corbis has identified a total of 232 images . . . in which it claims a copyright interest. Two of the images appeared on the IMDb *website*. The remaining 230 images have been copied, displayed, and sold by vendor defendants through their zShops *sites*." (emphasis added)).

[74] *See* 17 U.S.C. § 512(c)(1)(A) (2007).

storage was at the direction of the user.[75] In *ALS Scan*, ALS Scan alleged that the defendant was liable for infringing material posted in newsgroups by users.[76] The court did not even discuss the possibility that the infringing materials were not at the direction of the user.[77] In *Io Group, Inc. v. Veoh Networks, Inc.*, the court determined that even material created by a process initiated by a user upload is still considered at the direction of a user.[78] Veoh converted an uploaded file during the upload process.[79] The Northern District of California determined that even when an automated process gives rise to new infringing material, a service provider could still retain the safe harbor of section 512(c).[80] In addition to exempting service providers from liability arising out of potentially infringing material, Congress also wanted to protect service providers from acts that occurred automatically when a user transferred material to a service provider.[81] In *CoStar Group v. Loopnet*,[82] the District of Maryland held that a real estate listing site stored data at the direction of the user.[83] Loopnet allowed users to upload photos of real estate to a central server.[84] The service employed humans to scan photos for obvious acts of copyright infringement and other criteria.[85] The court

---

[75] *See, e.g.*, ALS Scan, Inc. v. RemarQ Cmtys., Inc., 239 F.3d 619, 623 (4th Cir. 2001) (ruling on a request for safe harbor under DMCA Section 512(c), the court never discussed whether the storage was at the direction of the user).

[76] *See id.* at 620 ("Two of the newsgroups to which RemarQ provides its subscribers access contain ALS Scan's name in the titles. These newsgroups-'alt.als' and 'alt.binaries.pictures.erotica.als'-contain hundreds of postings that infringe ALS Scan's copyrights. These postings are placed in these newsgroups by RemarQ's subscribers.").

[77] *See id.* at 623.

[78] *See* 586 F. Supp. 2d 1132, 1148 (N.D. Cal. 2008) ("[T]his court finds that Veoh does not lose safe harbor through the automated creation of these files.").

[79] *See id.* at 1147 ("[U]sing third-party software, its system creates the Flash and still-image files from user-submitted content.").

[80] *See id.* at 1148 ("But Veoh does not itself actively participate or supervise the uploading of files. Nor does it preview or select the files before the upload is completed. Instead, video files are uploaded through an automated process which is initiated entirely at the volition of Veoh's users.").

[81] H.R. REP. NO. 105-551, pt. 1, at 11 (1998) ("[L]iability is ruled out for passive, automatic acts engaged in through a technological process initiated by another.") [hereinafter *House Report*].

[82] 164 F. Supp. 2d 688 (D. Md. 2001).

[83] *Id.* at 702 ("[Pictures] are uploaded at the volition of the user.").

[84] *Id.* at 692 ("[A] user, usually a real estate broker, may post a listing of commercial real estate available for lease [and can] include a photograph.").

[85] *Id.* ("[Photos are] reviewed by a LoopNet employee to determine that it is in fact a photograph of commercial property and that there is no obvious indication

held that even though humans filtered data, users directed material to be stored with the service provider.[86] The court in *CoStar* further noted that "[t]he ability to remove or block access to materials cannot mean that those materials are not stored at the user's discretion or it would render the DMCA internally illogical."[87] Networks that rely on technology to filter or do not filter user-posted material certainly fit the standard of section 512(c) for materials posted at the direction of the user. Due to the broad language of section 512(c), a service provider that only provides storage for user material certainly stores material at the direction of the user.

¶30 A service provider will be able to call upon the section 512(c) safe harbor if it provides storage to a user and stores material at the direction of the user. Service providers in the hypothetical network provide storage for U0 at U0's discretion and do nothing except transfer the files to UF. The service provider does not screen data transferred to it, nor does it convert the data that U0 transfers to the service provider. Since the service providers in the hypothetical network store data at the direction of users, the service providers may benefit from the safe harbor of section 512(c).

E. Knowledge

¶31 To use the safe harbor, section 512(c) also requires that service providers lack knowledge of infringement. In the statute, there are three knowledge provisions:

> A service provider shall not be liable for … infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, 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.[88]

---

that the photograph was submitted in violation of LoopNet's terms and conditions.").

[86] *Id.* at 702 ("Although humans are involved rather than mere technology, they serve only as a gateway and are not involved in a selection process.").

[87] *Id.*

[88] 17 U.S.C. § 512(c)(1)(A) (2007).

¶32 The first and second provisions concern what the provider knows prior to an infringement suit. Section (iii) relates to the notification provided to a service provider by a rights holder.[89] Therefore, this portion of the iBrief will discuss section (i), section (ii), and will discuss section (iii) in light of the later discussion of notification.

1. Section (i)

¶33 Section (i) requires that, before invoking the safe harbor of section 512(c), a service provider lacked actual knowledge of infringement prior to the lawsuit.[90] Courts have set a high bar for actual knowledge and most providers simply have no idea when actual acts of infringement occur. In *Costar*, the plaintiff did not allege the service provider had actual knowledge even though humans scanned user-posted data for the service provider.[91] Even after notices of infringement were delivered to the defendant, the court did not impute actual knowledge to the defendant. In *CoStar*, defendant Loopnet's use of humans to filter material did not give rise to actual knowledge of infringement because "CoStar does not attach a copyright notice to its photos and even CoStar's own expert could not identify a CoStar photo simply by reviewing it."[92] The court held that unless the infringement was blatant, Loopnet would not obtain actual knowledge.[93] Since few service providers have actual knowledge, few cases discuss section (i). Most cases discuss the second section of the knowledge requirement in section 512(c).

2. Section (ii)

¶34 Section (ii) requires that, in order to use the safe harbor, in addition to not having actual knowledge, service providers must not be aware of "facts or circumstances" that indicate infringement.[94] The DMCA distinguishes section (ii) from cases in the physical realm that have imputed copyright infringement liability to auction houses under theories of secondary liability.[95] The House Report on the DMCA stated that "[t]his standard differs from existing law, under which a defendant

---

[89] *See infra* Part III.H.
[90] § 512(c)(1)(A)(i).
[91] *CoStar*, 164 F. Supp.2d at 698 ("Given the nature of the infringements in this case, it was impossible for LoopNet to have knowledge of the alleged infringement before receiving notice from CoStar.").
[92] *Id.* at 702 (explaining that although cursory, the service provider did have a human review uploaded content).
[93] *Id.* at 698 ("LoopNet cannot be charged with any form of knowledge before receiving claims of infringement from CoStar.").
[94] § 512(c)(1)(A)(ii).
[95] *House Report*, *supra* note 83, at 25 (1998).

may be liable for secondary infringement if it knows or should have known that material was infringing."[96] In *Fonovisa, Inc. v. Cherry Auction, Inc.*,[97] the Ninth Circuit held an auction house liable for copyright infringement on a theory of secondary liability under legal principles common prior to the DMCA.[98] The court reasoned that Cherry Auction was a proper target for secondary liability because Cherry Auction had the right to terminate users for any reason and those users sold infringing goods.[99] Similarly, eBay users transact business in goods that may infringe copyright.[100] In *Hendrickson v. eBay, Inc.*, however, the Central District of California held that postings on eBay do not give eBay knowledge of "facts or circumstances" that indicated infringement.[101] In contrast to *Cherry Auction*, the court held "that prior to [the] lawsuit, [eBay] did not have actual or constructive knowledge that particular listings were being used by particular sellers to sell pirated [videos]."[102] Therefore, the court allowed eBay to use the safe harbor of section 512(c).[103]

¶35 Congress intended that section (ii) work like a "red flag" test.[104] "The 'red flag' test has both a subjective and an objective element."[105] The subjective element asks what information the provider actually had.[106] The objective element then queries whether a reasonable person would have understood that information to point to infringement.[107] In

---

[96] *Id.*
[97] 76 F.3d 259 (9th Cir. 1996).
[98] *Id.* at 263 ("Cherry Action's ability to police it vendors under Cherry Auction's . . . broad contract with its vendors — was sufficient to satisfy the control requirement.").
[99] *Id.*
[100] Hendrickson v. eBay, Inc., 165 F.Supp. 2d 1082, 1087 (C.D. Cal. 2001) (noting that sellers post advertisements).
[101] *Id.* at 1088 ("Here, because the focus of the copyright claims against eBay concern infringing activity — the sale and distribution of pirated copies of "Manson"-using "materials" posted on eBay's website, Section 512(c) would provide eBay a safe harbor from liability if eBay meets the conditions set forth therein.").
[102] *Id*. at 1093.
[103] *Id.* at 1088.
[104] *Senate Report*, *supra* note 3, at 44 ("Section (c)(1)(A)(ii) can best be described as a 'red flag' test.").
[105] *Id.*
[106] *Id.* ("In determining whether the service provider was aware of a 'red flag,' the subjective awareness of the service provider of the facts or circumstances in question must be determined.").
[107] *Id.* ("[I]n deciding whether those facts or circumstances constitute a "red flag"-in other words, whether infringing activity would have been apparent to a

A&M Records, Inc. v. Napster, Inc.,[108] the Ninth Circuit held that Napster had knowledge of infringement occurring on its network.[109] Although *Napster* was decided under the broader secondary liability standard, the decision may factor into requests for the DMCA safe harbor. Napster's network likely would have met this "red flag" test. Looking through the lens of the "red flag" test, Napster had a list of the files transferred on its network, including many copyrighted popular music songs.[110] Napster therefore had information that indicated infringement (the subjective test) and the court held that a reasonable person probably would have understood that this information pointed to infringement (the objective test). In contrast with the standard articulated in *Napster*, however, the Senate Report on the DMCA stated that a, "service provider would have no obligation to seek out copyright infringement."[111] Although a service provider must acknowledge the "red flags" of infringement, the safe harbor of section 512(c) does not require that a service provider affirmatively search its network for potentially infringing material. Additionally, a service provider "would not qualify for the safe harbor if it had turned a blind eye to 'red flags' of obvious infringement."[112] In other words, the provider cannot be willfully blind of infringement.

3. Section (iii)

¶36 Section (iii) requires that once a service provider obtains knowledge of the infringement, the provider "expeditiously" remove infringing material.[113] This section imparts knowledge to a service provider after notification of infringement is presented to a service provider.[114] Therefore, only when a service provider receives a notification does section (iii) apply to the right to safe harbor under section 512(c). Part III. H. of this iBrief, below, discusses notification.

---

reasonable person operating under the same or similar circumstances-an objective standard should be used.").

[108]239 F.3d 1004 (9th Cir. 2001)

[109]*Id.* at 1021 ("Regardless of the number of Napster's infringing versus noninfringing uses, 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 of plaintiff's copyrights.").

[110] *Id.* at 1012 ("Once uploaded to the Napster servers, the user's MP3 file names are stored in a server-side "library" under the user's name and become part of a 'collective directory' of files available for transfer during the time the user is logged onto the Napster system.").

[111] *Senate Report*, *supra* note 3, at 48 (1998).

[112] *Id.*

[113] 17 U.S.C. § 512(c)(1)(A)(iii) (2009).

[114] *See infra* Part III.H.

4. Application

¶37 The service providers of the hypothetical network lack either actual knowledge or "facts or circumstances" that imply infringement. Without significant effort and the entire file, it would be impossible for the service providers to know the name of the file, let alone its contents. Therefore, unlike in *Napster*,[115] the service provider cannot simply search its indices to determine whether there is infringing content, even if that doctrine were applied in DMCA cases. Service providers cannot even search for files by original filename. Since the service providers do not know what files are being transferred, no red flags are presented to the service provider. In a sense, the service providers of the hypothetical network may be turning a blind eye to what data users transfer because they are unable to see what information is being stored. Service providers, however, must lack knowledge of the contents of network files, lest that information find its way into adverse hands. Therefore, the service providers should be able to moor in the safe harbor of section 512(c).

F. Right and Ability to Control

¶38 Section 512(c) also discusses a service provider's "right and ability to control [infringing] activity."[116] The right and ability to control activity is a necessary part of a rights holder's attempt to deny a service provider access to the safe harbor if the service provider gains a direct financial benefit from the activity.[117] There is a tension between this provision and the lack of knowledge requirement outlined in section 512(c)(1)(A).[118] For example, the Ninth Circuit held that Napster had the right and ability to control its users because "Napster has an express reservation of rights policy, stating on its website that it expressly reserves the 'right to refuse service and terminate accounts.'"[119] This interpretation of "right and ability to control," however, was not premised on section 512(c), but under the more expansive general secondary infringement standard.[120] Considering this tension, the

---

[115] *See* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1024 (9th Cir. 2001) ("Napster, however, has the ability to locate infringing material listed on its search indices. . . .").

[116] § 512(c)(1)(B).

[117] *Id.*; *see also supra* Part III.E.

[118] *See* Corbis Corp. v. Amazon.com, Inc., 351 F.Supp. 2d 1090, 1110 (W.D. Wash. 2004) (discussing how other courts have held the ability to terminate accounts is not tantamount to the right and ability to control).

[119] *A&M Records*, 239 F.3d at 1023 (agreeing with the lower court that since Napster policed its service, it had the right and ability to control users).

[120] *Id.* at 1024 ("Napster's failure to police the system's 'premises' . . . leads to the imposition of vicarious liability.").

Central District of California has held that it would be impossible to satisfy both the termination procedure of section 512(c)(1)(A)(iii) and lack a right and ability to terminate accounts.[121] The court went on to note that "Congress could not have intended for courts to hold that a service provider loses immunity under the safe harbor provision of the DMCA because it engages in acts that are specifically required by the DMCA."[122] A service provider with a termination policy that satisfies section 512(c)(1)(A)(iii) does not necessarily mean that the service provider has the right and ability to control users.

¶39 This iBrief argues that, in the hypothetical network, the service providers have a valid termination policy. Beyond that, however, the service providers do nothing to control network access. Since the service providers do no more than enforce the termination policy, the service providers do not have the right and ability to control material on its network. Therefore, the service providers should retain the safe harbor of section 512(c).

G. Financial Benefit

¶40 If a service provider does not have the right and ability to control infringing activity, the service provider can use the safe harbor of section 512(c) regardless if the service provider obtains a financial benefit from the infringement.[123] If a service provider has the right and ability to control activity or material on its network, however, the service provider can only use the section 512(c) safe harbor if the service provider does not "[derive] a direct financial benefit from the infringement."[124] In addition to obvious examples like subscription fees or paying for access to infringing materials, direct financial benefit includes what consists of a "draw" to a service provider.[125] The Senate Report describes a draw as "any such fees where the value of the service lies in providing access to

---

[121] Hendrickson v. eBay, Inc., 165 F.Supp. 2d 1082, 1093 (C.D. Cal. 2001) ("[T]he 'right and ability to control' the infringing activity, as the concept is used in the DMCA, cannot simply mean the ability of a service provider to remove or block access to materials posted on its website or stored in its system. To hold otherwise would defeat the purpose of the DMCA and render the statute internally inconsistent.").

[122] *Id*. at 1093–94.

[123] *See Corbis*, 351 F.Supp. at 1110 ("Because Amazon does not have the right and ability to control the infringing material, it is not necessary for this Court to inquire as to whether Amazon receives a direct financial benefit from the allegedly infringing conduct.").

[124] Ellison v. Robertson, 357 F.3d 1072, 1078 (9th Cir. 2004).

[125] *Id.* at 1079 ("Thus, the central question of the 'direct financial benefit' inquiry in this case is whether the infringing activity constitutes a draw for subscribers, not just an added benefit.").

infringing material."[126] In *Ellison v. Robertson*, the Ninth Circuit held that America Online's (AOL) USENET service did not retain subscribers or result in new subscribers.[127] The court held that there was no direct financial benefit to the provider because the infringing activity did not add to AOL's bottom line.[128] Therefore, to retain safe harbor status, the infringing material or activity cannot be the reason users choose a certain service provider, if the service provider charges a subscription fee. The Ninth Circuit has also held that, where the presence of material or activity increases users and thereby increases advertising revenue, the service provider derives a direct financial benefit from that material or activity.[129] That holding, however, was in *Napster*, where the Ninth Circuit ruled under the broader standards of general secondary liability.[130] Without any revenue or expected revenue, a service provider does not obtain any sort of financial benefit.

¶41 If service providers were required to host files in order to download files, there would arguably be a benefit to the service providers. The ability to download free copies of copyrighted materials may satisfy the financial benefit standard because there would otherwise be a cost to access that material. The hypothetical network disassociates uploads from downloads and no benefits accrue to service providers. As long as the service providers internalize the costs of running the network and receive no outside income in connection with running the network, the service providers would not obtain any financial benefit from infringing activity or material. Since the service providers in the hypothetical network derive neither explicit financial benefit nor a privilege by storing material, the service providers derive no direct

---

[126] *Senate Report*, *supra* note 3, at 45 (1998).

[127] *Ellison*, 357 F.3d at 1079 ("We note that there is no evidence that indicates that AOL customers either subscribed because of the available infringing material or canceled subscriptions because it was no longer available.").

[128] *Id.* ("The record lacks evidence that AOL attracted or retained subscriptions because of the infringement or lost subscriptions because of AOL's eventual obstruction of the infringement. Accordingly, no jury could reasonably conclude that AOL received a direct financial benefit from providing access to the infringing material.").

[129] A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1023 (9th Cir. 2001) ("Financial benefit exists where the availability of infringing material 'acts as a 'draw' for customers.'" (citing Fonovisa Inc. v. Cherry Auction, Inc., 76 F.3d 259, 263–64 (9th Cir. 1996))).

[130] *Id.* at 1024 ("Napster, however, has the ability to locate infringing material listed on its search indices, and the right to terminate users' access to the system. . . . Our review of the record requires us to accept the district court's conclusion that plaintiffs have demonstrated a likelihood of success on the merits of the vicarious copyright infringement claim.").

financial benefit from the infringing materials stored on the network. Therefore, the service providers may use the safe harbor of section 512(c) because they do not derive a financial benefit from running the network.

H. Notification

¶42 Finally, section 512(c)(1) requires that service providers accept notifications from rights holders.[131] These notifications inform service providers of infringing activity or material.[132] If a rights holder does not present a notification prior to filing a suit for copyright infringement, a service provider is free to use the safe harbor at trial to disclaim liability.[133] The section states that, "upon notification of claimed infringement as described in paragraph (3), [the service provider must respond] expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity."[134] The referenced provision, section 512(c)(3), sets forth the notification requirements.[135] There are several notification provisions, but for the purposes of the hypothetical network, the important notice requirement is section 512(c)(3)(A)(iii). Section 512(c)(3)(A)(iii) requires that the notification include: "[i]dentification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material."[136] Essentially, for a notification to be proper, a rights holder must identify infringing material and the location of that material.[137]

¶43 The rights holder does not need to follow the strictures of the notification procedure; substantially compliant notification imparts knowledge to the service provider and creates liability for a service provider that does not acquiesce to the notification by removing infringing material.[138] The statute requires identification of a specific

---

[131] 17 U.S.C. § 512(c)(1)(C) (2009).
[132] *Id.*
[133] Corbis Corp. v. Amazon.com, Inc., 351 F.Supp. 2d 1090, 1107 (W.D. Wash. 2004) ("Corbis, of course, was under no obligation to file notice of claimed infringement before filing this suit.").
[134] § 512(c)(1)(C).
[135] § 512(c)(3).
[136] § 512(c)(3)(A)(iii).
[137] *Id.*
[138] *See* 17 U.S.C. § 512(c)(1)(C); Corbis Corp. v. Amazon.com, Inc., 351 F.Supp. 2d 1090, 1107 (W.D. Wash. 2004) ("[Corbis's] decision to forego the DMCA notice provisions, however, stripped it of the most powerful evidence of

location of infringing material or activity,[139] but there are at least two cases where specific identification is not required. First, when virtually all of a network resource is infringing—such as a website—a rights holder need only identify that resource.[140] In *ALS Scan*, the court held that the plaintiff had indeed provided sufficient information to locate infringing material by "assert[ing] that virtually all of the images at the two sites were its copyrighted material."[141] The court held that "when a letter provides notice equivalent to a list of representative works that can be easily identified by the service provider, the notice substantially complies with the notification requirements."[142]

¶44 Second, specific identification may not be required when the service provider can easily search for infringing material.[143] In *Hendrickson*, the Central District of California held that a rights holder did not give eBay sufficient notice where the plaintiff only stated that pirated copies of his movie were being sold on eBay.[144] Since he did not identify where the infringing material was located, the court ruled that the notification was insufficient.[145] It noted that, however, like in *ALS Scan*, "there may be instances where a copyright holder need not provide eBay with specific item numbers to satisfy the identification requirement."[146] The court assumed that eBay could search for infringing material given enough information.[147] The notification must

---

a service provider's knowledge—actual notice of infringement from the copyright holder.").

[139] § 512(c)(3)(A)(iii).

[140] ALS Scan, Inc. v. Remarq Comtys., Inc., 239 F.3d 619, 625 (4th Cir. 2001) ("ALS Scan . . . asserted that virtually all the images at the two sites were its copyrighted material . . . [and] ALS Scan substantially complied with the notification requirement.").

[141] *Id.*

[142] *Id.*

[143] Hendrickson v. eBay, Inc., 165 F.Supp. 2d 1082, 1090 (C.D. Cal. 2001) ("[I]f a movie studio advised eBay that all listings offering to sell a new movie (e.g., ``Planet X,") that has not yet been released in VHS or DVD format are unlawful, eBay could easily search its website using the title ``Planet X" and identify the offensive listings.").

[144] *Id.* ("[Plaintiff] merely assert that pirated copies of 'Manson' DVDs were being sold on eBay . . . Plaintiff's e-mail did not identify the basis for his claim that the seller was selling a pirated copy of 'Manson.'").

[145] *Id.* at 1092 ("[P]roper identification under Section 512(c)(3)(A)(iii) should include the specific item numbers of the listing that are allegedly offering pirated copies of "Manson" for sale.").

[146] *Id.* at 1090.

[147] *Id.* at 1090 ("eBay could easily search its website using the title 'Planet X' and identify the offensive listings.").

denote, with some specificity, which files are infringing. If a rights holder was unable to show that virtually all the data on the network is infringing (like in *ALS Scan*) or point to specific acts of infringement (like in *Hendrickson*), notification would be insufficient.

¶45 In the hypothetical network, service providers only hold pieces of encrypted data. Moreover, due to the encoding procedure, only users with an encoding key can translate the file pieces into the original encrypted file. Note that if a dictatorial regime could easily scan for files, the utility of the network would be defeated. Therefore, in the hypothetical network, infringing files can only be found by trusted users. Since only trusted users can find files, a rights holder would not have a way to determine the location of files that infringe its copyright. Furthermore, the file pieces are not recognizable unless combined to create a full file. Thus, even if a rights holder did scan for and download file pieces, upon which there are no restrictions, the rights holder would be unable to determine if a certain file contained its copyrighted material. Therefore, the rights holder could not determine which copyrighted work the file infringed.

¶46 Each service provider only holds one of part of a file; hence, it is impossible for a service provider to store an infringing file. First, it is not possible for a rights holder to show what work is being infringed. When the data is encrypted and broken up, an individual part does not infringe on any work (at least to the extent that it does not accidentally transform the scrambled part into another copyrighted work). Second, although a rights holder is allowed to search the network, the rights holder would have to be trusted with an encoding key to obtain the names of the file parts that constitute an original file. In practice, a rights holder could not determine the location of infringing files. Since the rights holder cannot determine which copyright a file infringes and the locations of files that infringe that work, the rights holder could not present a service provider with proper notification and, without proper notification, the service provider will never need to "expeditiously" remove infringing material as required in section (iii) of the knowledge provision.[148]

IV. OTHER BODIES OF LAW

¶47 This iBrief has argued that the service providers of the hypothetical network can tack gracefully into the safe harbor of section 512(c). Recent cases have indicated that potential service providers of the hypothetical network should consider the implication of liability based on bodies of law outside the safe harbor of section 512(c).

---

[148] *See supra* Part III.E.

¶48 Courts have held that certain providers exceeded the bounds of section 512 and were not privy to its safe harbor.[149] In *Aimster*, for example, obvious infringement occurred and the service provider knew of the infringement.[150] *Aimster* used the -ster ending for its network (echoing Napster), and affirmatively taught users how to infringe copyright on their network.[151] In response, the Seventh Circuit spent little time dismissing the network operator's ability to moor in the safe harbor of section 512.[152] Similarly, the Supreme Court has held that networks may be liable for less obvious copyright infringement on a theory of inducement.[153] In *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, the Court created this new theory of copyright liability.[154] Grokster and StreamCast actively promoted infringement on their networks.[155] The Court held that the companies were liable for the infringement of their users because "[t]he classic instance of inducement is by advertisement or solicitation that broadcasts a message designed to stimulate others to commit violations."[156] The decision premised liability on affirmative acts: "Grokster and StreamCast are not, however, merely passive recipients of information about infringing use. . . . Each took active steps to encourage infringement."[157] Moreover, the Court held that "mere knowledge of infringing potential or of actual infringing uses would not

---

[149] *In Re* Aimster Copyright Litig., 334 F.3d 643, 655 (7th Cir. 2003) ("[In contrast with the intent of the DMCA,] Aimster invited [users to infringe copyright], showed them how they could do so with ease using its system, and by teaching its users how to encrypt their unlawful distribution of copyrighted material has disabled itself from doing anything to prevent infringement.").
[150] *Id.*
[151] *Id.*
[152] *Id.*
[153] Metro-Goldwyn-Mayer Studios, Inc. V. Grokster, Ltd., 545 U.S. 913, 936–37 (2005) ("[T]he inducement rule, too, is a sensible one for copyright. We adopt it here, holding 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.").
[154] *Id*. at 936 ("For the same reasons that Sony took the staple-article doctrine of patent law as a model for its copyright safe-harbor rule, the inducement rule, too, is a sensible one for copyright.").
[155] *Id.* at 938 ("[B]oth companies communicated a clear message by responding affirmatively to requests for help in locating and playing copyrighted materials.").
[156] *Id.* at 937.
[157] *Id.* at 923–24.

be enough here to subject a distributor to liability."[158] Therefore, passive activity does not give rise to a claim of inducement.

¶49 In the hypothetical network, the service providers do not advertise or provide any service to users, except storage. The *Grokster* decision premised liability on affirmative acts.[159] Therefore, the inducement liability created in *Grokster* is inapplicable to the hypothetical network's service providers. Moreover, the service providers in the hypothetical network have no idea what data is passing through their machines. The service providers would not know that infringing activity was occurring on the network, in contrast with most file sharing systems. Courts should not impose a new theory of liability because the hypothetical network respects both the letter and the overall spirit of section 512.

CONCLUSION

¶50 What if a service operated completely within the confines of section 512, yet allowed for unbridled copyright infringement? This iBrief has outlined such a potential network. Each service provider has a policy to terminate users and implements that policy, but is unlikely to enforce it.[160] The service providers do not frustrate standard technical measures.[161] The service providers provide storage at the direction of users.[162] The service providers have neither knowledge nor reasonable possibility of knowledge of infringement.[163] The service providers do not have a right or ability to control the users of the network,[164] nor receive any financial benefit in connection with the network.[165] There is a small likelihood a rights holder could serve a notice on a service provider that would give them knowledge of infringing activity or material on the network.[166] A potential chink in this hypothetical is that a service provider in this potential network is a single user. Although there is no statutory floor on the size of a service provider, a court may hold that Congress did not intend to allow the service provider definition to apply to individuals.[167] Furthermore, a court may hold this

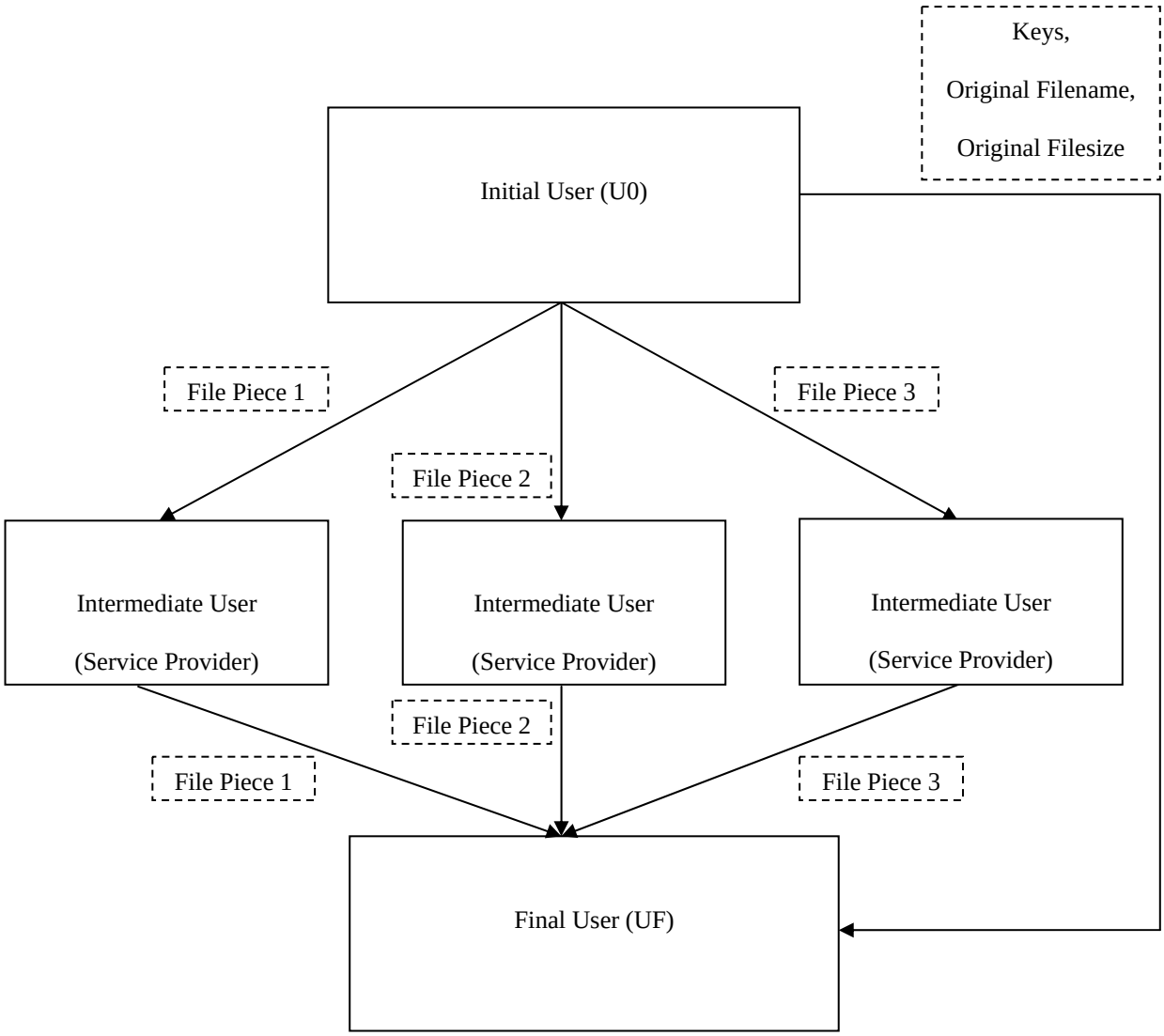
---

[158] *Id.* at 937.
[159] *Grokster*, 545 U.S. at 923–24.
[160] *See supra* Part III.B.
[161] *See supra* Part III.C.
[162] *See supra* Part III.D.
[163] *See supra* Part III.E.
[164] *See supra* Part III.F.
[165] *See supra* Part III.G.
[166] *See supra* Part III.H.
[167] *See supra* Part III.A.

hypothetical network illegal because of the potential for unbridled infringement.

¶51 This iBrief has argued that supporters of a hypothetical network will not be liable under secondary liability theories of copyright infringement. The network assumes these supporters will retain pieces of files to ease information transfer among members of a group. The network was designed to ensure unbridled transfer of information—for example, information that may otherwise be censored or monitored through normal communication channels of dictatorial governments. Therefore, the author hopes this hypothetical network will be used to encourage activities of oppressed minorities, specifically those seeking political communication. Paradoxically, even if these supporters hold files that infringe copyright, the supporters may still benefit from the broad safe harbor within section 512 of the DMCA.

APPENDIX


Keys,
Original Filename,
Original Filesize
Initial User (U0)
File Piece 1
File Piece 2
File Piece 3
Intermediate User
(Service Provider)
Intermediate User
(Service Provider)
Intermediate User
(Service Provider)
File Piece 2
File Piece 1
File Piece 3
Final User (UF)