DMCA SAFE HARBORS FOR VIRTUAL PRIVATE SERVER PROVIDERS HOSTING BITTORRENT CLIENTS

STEPHEN J. WANG[†]

ABSTRACT

By the time the U.S. Supreme Court decided Metro-Goldwyn-Mayer Studios Inc. v. Grokster Ltd. in 2005, Internet users around the globe who engaged in copyright infringement had already turned to newer, alternative forms of peer-to-peer filesharing. One recent development is the "seedbox," a virtual private server rentable for use to download and upload ("seed") files through the BitTorrent protocol. Because BitTorrent is widely used for both non-infringing and infringing purposes, the operators of seedboxes and other rentable BitTorrent-capable virtual private servers face the possibility of direct and secondary liability as did the defendants in Grokster and more recent cases like UMG Recordings, Inc. v. Shelter Capital Partners LLC and Viacom Intern., Inc. v. YouTube, Inc. This Issue Brief examines whether the "safe harbor" provisions of the Digital Millennium Copyright Act (DMCA) may shield virtual private server providers with customers running BitTorrent clients from potential liability for copyright infringement. It argues that general virtual private server providers are likely to find refuge in the safe harbor provisions as long as they conscientiously comply with the DMCA. In contrast, virtual private server providers specifically targeting BitTorrent users ("seedbox providers") are much less likely to receive DMCA safe harbor protection.

INTRODUCTION

The distribution of large files, from movies to research data, has never been easier or more prevalent than it is today. In 2011, Netflix's movie streaming service accounted for 22.2 percent of all download traffic through wired systems in North America.[1] BitTorrent, a filesharing

---

[†] J.D. Candidate, 2014, Duke University School of Law; B.A. in Political Science and Asian Studies, 2011, Rice University. The author would like to thank Professor Jennifer Jenkins, a fellow Rice Owl, for her guidance in preparing this Issue Brief.

[1] Matthew Lasar, *Netflix Now "the King" of North American Internet Traffic*, ARS TECHNICA (May 17, 2011, 11:21 PM), http://arstechnica.com/tech-

protocol, followed closely behind with a still enormous share of 21.6 percent,[2] and in 2004, one report found that BitTorrent accounted for 35 percent of all Internet traffic.[3] The protocol's popularity rests on its facilitation of file distribution without the traditional resource constraints of centralized distribution.[4]

Internet users and companies wanting to distribute large content previously faced the high costs of operating or renting a server from which every individual would download a file or group of files.[5] Now, with BitTorrent, peers download different parts of a file from each other simultaneously; BitTorrent bypasses the need for a central server to feed data to every potential downloader.[6]

At least a handful of BitTorrent users seeking to further increase their downloading and uploading power have begun using "seedboxes" — BitTorrent clients running on rented virtual private servers (VPS).[7] Some providers of these virtual private servers actually specialize in hosting BitTorrent ("seedbox providers"),[8] whereas most offer virtual private servers more neutrally ("general VPS providers"), not marketing to the narrower group of BitTorrent-using customers.[9]

Like MP3tunes in *Capitol Records, Inc. v. MP3tunes, LLC*,[10] VPS providers, by hosting customers' private, potentially infringing content, face potential liability for copyright infringement. In the event of consequent

---

policy/2011/05/netflix-now-owns-almost-30-percent-of-north-american-fixed-internet-traffic/.

[2] *Id.*

[3] *In Praise of P2P*, THE ECONOMIST, Dec. 4, 2004, at 29.

[4] *See id*; *see also* Eric Bangeman, *BitTorrent Moves Further into the Mainstream*, ARS TECHNICA (Mar. 17, 2004, 10:49 AM), http://arstechnica.com/uncategorized /2004/03/3535-2/ (providing early examples of companies using BitTorrent to effectively reduce the cost of distributing large amounts of data).

[5] *In Praise of P2P*, *supra* note 3.

[6] *Id.*

[7] Sebastian Anthony, *Faster Torrenting with a VPS Seedbox*, EXTREME TECH (Apr. 29, 2011, 12:00 PM), http://www.extremetech.com/computing/84240-faster-torrenting-with-a-vps-seedbox.

[8] *See, e.g.*, SEEDBOXHOSTING.COM, https://www.seedboxhosting.com (last visited Nov. 18, 2012); SUPERSEEDBOX, http://superseedbox.com (last visited Nov. 18, 2012); PULSED MEDIA, http://pulsedmedia.com (last visited Nov. 18, 2012); SEED UNLIMITED, https://www.seedunlimited.com (last visited Nov. 18, 2012).

[9] *See, e.g.*, *Virtual Private Server*, OVH.CO.UK, http://www.ovh.co.uk/vps/ (last visited Nov. 18, 2012); EVOBOXES, https://evoboxes.org (last visited Nov. 18, 2012); DOTBLOCK, http://www.dotblock.com (last visited Nov. 18, 2012); LINODE.COM, http://www.linode.com (last visited Nov. 18, 2012).

[10] Capitol Records, Inc. v. MP3tunes, LLC, 821 F. Supp. 2d 627 (S.D.N.Y. 2011).

litigation, they would seek protection from liability using the "safe harbor" provisions of the Digital Millennium Copyright Act[11] (DMCA). Although the trade organizations of the film and recording industries have yet to actively battle VPS and seedbox providers for allowing BitTorrent use, the possibility of litigation is rapidly increasing as costs for renting virtual servers decrease[12] and filesharers fleeing Internet service providers' new experimental "six strikes schemes"[13] move their infringing activities to remote servers. It would not be the first time those groups have litigated against BitTorrent-related servers and sites,[14] but, with the Second Circuit's recent groundbreaking decision in *Viacom Intern., Inc. v. YouTube, Inc*,[15] the particular issue of safe harbor for seedbox providers presents a novel twist.

This Issue Brief first provides background on BitTorrent as well as seedboxes and general VPS providers operating BitTorrent clients. It then explores the current contours of the most relevant DMCA safe harbor provisions before applying the DMCA analysis to seedbox and general VPS providers. This Brief concludes that, as long as they conscientiously comply with the particular DMCA rules, general virtual private server providers should successfully avoid liability for their customers' infringing uses; however, seedbox providers are unlikely to receive safe harbor protection.

I. BITTORRENT AND SEEDBOXES

BitTorrent introduced a model of filesharing completely different from its predecessors. Whereas Napster and its immediate successors—such as Grokster, KaZaA, and Morpheus—all provided a one-stop filesharing search box, BitTorrent, as a protocol, only provides the mechanisms that any group of people can utilize to efficiently distribute files between them. The group using BitTorrent could be public or private, but BitTorrent's effectiveness relies on a group of users downloading and uploading a particular "torrent" simultaneously; every user connected to a server

---

[11] Digital Millennium Copyright Act, 17 U.S.C. § 512 (2006).

[12] G.F., *The End of a Faithful Server*, ECONOMIST (Nov. 23, 2010, 6:47 PM), http://www.economist.com/node/21013174.

[13] *See* Joe Mullin, *How ISPs Will Do "Six Strikes": Throttled Speeds, Blocked Sites*, ARS TECHNICA (Nov. 16, 2012, 10:06 AM). "Six strikes" refers to Internet service providers' programs for initially warning customers caught infringing copyrights and for applying progressively greater penalties after repeated infringement.

[14] *See* Eric Bangeman, *TorrentSpy Ordered to Pay $110 Million in Damages to MPAA*, ARS TECHNICA (May 7, 2008, 4:24 PM) for one major lawsuit against a formerly popular BitTorrent tracker.

[15] *See* Viacom Intern., Inc. v. YouTube, Inc., 676 F.3d 19 (2d Cir. 2012).

("tracker") for a particular torrent downloads from each other. But there is no centralized tracker, and a tracker can be created and set up by anyone with the necessary knowledge. The author of the BitTorrent protocol has, in effect, set loose on the world a content-neutral file distribution technology that anyone can use—just as the HTTP protocol creates the fabric for both lawful[16] and illicit uses of the Internet and the Web. As a neutral technological specification, BitTorrent is likely to itself remain on legally solid ground.[17] However, operators of particular BitTorrent trackers and websites promoting infringement have been and continue to be the target of legal action.[18] In fact, anyone substantively facilitating illicit use of BitTorrent could possibly be sued under secondary liability theories.[19]

Although BitTorrent is designed for use on personal systems, many users have turned to operating BitTorrent on remote computers, often residing in hosting facilities. BitTorrent users do this for a number of reasons. The protocol's mechanisms notably reward users whose computers

[16] *See* Bangeman, *supra* note 4 (providing the examples of computer game developers Valve and Blizzard as early commercial adopters of BitTorrent to facilitate authorized distribution of their own software); Matthew Helton, *Secondary Liability for Copyright Infringement BitTorrent as a Vehicle for Establishing a New Copyright Definition for Staple Articles of Commerce*, 40 COLUM. J.L. & SOC. PROBS. 1, 2 (2006) (offering the examples of film director Peter Jackson using BitTorrent to generate interest in one of his films as well as the National Aeronautics Space Administration using BitTorrent to effectively distribute some of their large image files).

[17] *See* Alvin Chan, *The Chronicles of Grokster: Who Is the Biggest Threat in the P2P Battle?*, 15 UCLA ENT. L. REV. 291, 300 (2008) (noting that the "academic consensus" believes BitTorrent safe post-*Grokster*). *But see* Rebecca Giblin, *A Bit Liable - A Guide to Navigating the U.S. Secondary Liability Patchwork*, 25 SANTA CLARA COMPUTER & HIGH TECH. L.J. 7, 48 (2008) (concluding that, although "BitTorrent, Inc. is unlikely to be held secondarily liable for its users' infringements," the law still offers similar technological innovators little comfort).

[18] *See*, *e.g.*, David Kravets, *Oink Admin Beats File Sharing Charges*, WIRED (Jan. 15, 2010, 1:21 PM), http://www.wired.com/threatlevel/2010/01/oink-admin-beats-file-sharing-charges/ (discussing the trial of a private BitTorrent tracker administrator in British court); Michael A. Lindenberger, *Internet Pirates Face Walking the Plank in Sweden*, TIME, Feb. 20, 2009, *available at* http://www.time.com/time/business/article/0,8599,1880981-3,00.html (discussing the now-resolved suit filed against the operators of the popular Swedish BitTorrent site The Pirate Bay).

[19] *See* Bryan H. Choi, *The Grokster Dead-End*, 19 HARV. J.L. & TECH. 393, 408 (2006) (discussing the vulnerability of BitTorrent-related sites to legal pressure). *See generally* Lital Helman, *Pull Too Hard and the Rope May Break: On the Secondary Liability of Technology Providers for Copyright Infringement*, 19 TEX. INTELL. PROP. L.J. 111 (2010) (considering the secondary liability of BitTorrent tracker servers among other services after *Grokster*).

upload generously, with greater priority for downloading from other users downloading the same thing.[20] Moreover, private BitTorrent trackers often reward registered users who upload more data to others.[21] Thus, operating BitTorrent on a computer connected to the Internet with much faster speeds than a home connection offers great advantages in terms of downloading power by way of increased uploading power.[22] Furthermore, remotely operating a BitTorrent client offers an additional level of anonymity guarding against potential trouble with Internet service providers, including universities, who may receive infringement notices from copyright holders.[23]

Although there are services that market themselves explicitly as providing seedboxes,[24] there remains a wide range of "neutral" virtual private servers that can be used for anything, including operating a remote BitTorrent client.[25] These differ minimally from traditional web hosting packages,[26] which provide space to serve content accessible on the Web and allow operating related applications. Indeed, many VPS providers sell traditional web hosting as well.[27]

The different characteristics of seedbox and general VPS providers present interesting questions of liability. Although BitTorrent itself is a

---

[20] *In Praise of P2P*, *supra* note 3, at 29-30.

[21] *10 Reasons Why You Need a Seedbox*, FILESHAREFREAK (May 1, 2008), http://filesharefreak.com/2008/05/01/10-reasons-why-you-need-a-seedbox.

[22] *Id.*

[23] *Id.*; *see also* Sara Lipka, *RIAA Drops Lawsuits But Keeps the "Takedown" Notices Coming*, THE CHRONICLE OF HIGHER EDUCATION (Feb. 4, 2009, 4:13 PM), http://chronicle.com/blogs/wiredcampus/riaa-drops-lawsuits-but-keeps-the-takedown-notices-coming/4511 for an example of copyright holders sending universities takedown notices for their students' alleged infringement.

[24] *See, e.g.*, SEEDBOXHOSTING.COM, https://www.seedboxhosting.com (last visited Nov. 18, 2012); SUPERSEEDBOX, http://superseedbox.com (last visited Nov. 18, 2012); PULSED MEDIA, http://pulsedmedia.com (last visited Nov. 18, 2012); SEED UNLIMITED, https://www.seedunlimited.com (last visited Nov. 18, 2012).

[25] *See, e.g.*, *Virtual Private Server*, OVH.CO.UK, http://www.ovh.co.uk/vps/ (last visited Nov. 18, 2012); EVOBOXES, https://evoboxes.org (last visited Nov. 18, 2012); DOTBLOCK, http://www.dotblock.com (last visited Nov. 18, 2012); LINODE.COM, http://www.linode.com (last visited Nov. 18, 2012). *But see VPS Terms of Service*, HostGator, http://www.hostgator.com/tos/vps-tos.php (last visited Nov. 18, 2012) for an example of a particularly cautious virtual private server provider who has opted to expressly prohibit BitTorrent use.

[26] *See* G.F., *supra* note 12 (explaining the uses and practicalities of virtual private servers, typical shared web hosting, and cloud servers).

[27] *See, e.g.*, *Web Hosting Offers*, OVH.CO.UK, http://www.ovh.co.uk/web-hosting (last visited Nov. 18, 2012) (OVH offers both web hosting and VPS services, as do many VPS providers).

neutral technology, and much of overall BitTorrent use is non-infringing,[28] some of the BitTorrent use on seedboxes may infringe on copyrights. And most seedbox providers appear not to strive for DMCA compliance.[29] General VPS providers, on the other hand, often strive for DMCA safe harbor compliance and may consequently avoid direct and secondary liability more easily.[30]

II. THE DIGITAL MILLENNIUM COPYRIGHT ACT SAFE HARBORS

Because the potential for strict liability copyright infringement would have otherwise severely chilled the promise of the Internet,[31] Congress enacted 17 U.S.C. § 512[32] of the Digital Millennium Copyright Act (DMCA) to "create a series of 'safe harbors[]' for certain common activities of service providers."[33] Different kinds of service providers may gain protection from secondary liability for copyright infringement by meeting both threshold statutory requirements and the statutory requirements particular to the kind of service. Section 512(c) provides the best fit for seedbox and general VPS providers. However, like other parts of the DMCA, case law has yet to fully define § 512(c)'s particularities.[34]

---

[28] Choi, *supra* note 19, at 407 (stating that "BitTorrent has arguably demonstrated sufficient noninfringing uses, even under the more stringent standard favored by Justice Ginsburg and the Seventh Circuit . . .").

[29] *See, e.g.*, *Terms of Service*, SEEDUNLIMITED, https://www.seedunlimited.com/tos.php (last visited Nov. 18, 2012) (stating that users may not store unauthorized copyrighted material but not mentioning the DMCA or a designated agent for notices); SEEDBOXHOSTING.COM, https://www.seedboxhosting.com/ (last visited Nov. 18, 2012) (not showing any effort to mitigate potential copyright infringement by users). *But see DMCA Policy*, SEEDSTUFF, http://seedstuff.ca/dmca.php (last visited Nov. 18, 2012) as an example of a seedbox provider with a public DMCA policy, including a designated copyright agent.

[30] *See, e.g.*, *Terms of Service*, DOTBLOCK, http://www.dotblock.com/terms.php (last visited Nov. 18, 2012) (stating specifically that DotBlock has a responsibility to comply with DMCA complaints); *Terms of Service*, LINODE.COM, http://www.linode.com/tos.cfm (last visited Nov. 18, 2012) (stating more generally that Linode will take action upon receiving notices of violation of United States or international copyright law).

[31] *See* 144 Cong. Rec. S11,889 (daily ed. Oct. 2, 1998) (statement of Sen. Hatch) (explaining that Congress wanted to provide reassurance "in order to attract the substantial investments necessary to continue the expansion and upgrading of the Internet").

[32] 17 U.S.C. § 512 (2006).

[33] Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 27 (2d Cir. 2012) (quoting S.Rep. No. 105-190 at 2 (1998)).

[34] *See* 17 U.S.C. § 512(c).

A. DMCA Safe Harbor Statutory Basics

The safe harbor provisions § 512(a)–(d) define the four kinds of service providers who qualify for safe harbor protection from secondary liability—"(a) transitory digital network communications, (b) system caching, (c) information residing on systems or networks at [the] direction of users, and (d) information location tools."[35] Examples of services qualifying under § 512(a) include actual Internet service providers, who provide "dumb pipes" generally not discriminating between different types of Internet data packets, or conduits temporarily storing data.[36] Section 512(b) includes service providers that may temporarily and automatically cache data for a variety of reasons.[37] Services potentially eligible for § 512(c) protection include web hosting providers, video hosting sites such as YouTube and Veoh, and cloud and other online storage providers[38] such as Dropbox, Amazon Cloud Drive, Google Drive, and Apple iCloud.[39] Finally, § 512(d) might offer safe harbor to search engines like Google Search and Microsoft Bing.[40]

1. Service Provider Definition

Courts must begin DMCA safe harbor analyses with the threshold requirement of meeting the definition of "service provider" set by § 512(k).[41] For § 512(a), § 512(k)(1)(A) defines "service provider" as "an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received."[42] For § 512(b)–(d), § 512(k)(1)(B) more broadly defines "service provider" as "a provider of online services or

---

[35] *Id.* (citing 17 U.S.C. § 512(a)-(d)) (quotation marks omitted).

[36] *See* 17 U.S.C. § 512(a). *See also* Ellison v. Robertson, 357 F.3d 1072, 1081 (9th Cir. 2004) (holding that a service provider's automated storing of USENET newsgroup material for fourteen days was sufficiently "transient" and "intermediate" to maintain § 512(a) safe harbor qualification).

[37] *See* 17 U.S.C. § 512(b). *See also* Field v. Google Inc., 412 F. Supp. 2d 1106, 1123–25 (D.Nev. 2006) (holding that Google's automated caching of websites fit the § 512(b) safe harbor requirements).

[38] 17 U.S.C. § 512(c); *see* Brandon J. Trout, *Infringers or Innovators? Examining Copyright Liability for Cloud-Based Music Locker Services*, 14 VAND. J. ENT. & TECH. L. 729, 739 (2012) for an overview of some services likely falling under 512(c) protection.

[39] *See* 17 U.S.C. § 512(c).

[40] *See, e.g.*, Perfect 10, Inc. v. Amazon, Inc., 508 F.3d 1146, 1175 (9th Cir. 2007).

[41] 17 U.S.C. § 512(k).

[42] 17 U.S.C. § 512(k)(1)(A).

network access, or the operator of facilities therefor, and includes an entity described in subparagraph (A)."[43]

2. Repeat Infringer Policy Requirement

Next, § 512(i) requires the service provider to maintain a "repeat infringer policy,"[44] outlined by § 512(i):

(i) Conditions for Eligibility.—

(1) Accommodation of technology.—The limitations on liability established by this section shall apply to a service provider only if the service provider—

(A) 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; and

(B) accommodates and does not interfere with standard technical measures.[45]

In its important *Capitol Records, Inc. v. MP3tunes, LLC* decision, the Southern District of New York followed the Ninth Circuit's interpretation of § 512(i), holding that "implementation is reasonable if the service provider (1) has a system for responding to takedown notices, (2) does not interfere with the copyright owners' ability to issue notices, and (3) under 'appropriate circumstances' terminates users who repeatedly or blatantly infringe copyrights."[46] It further explained that § 512(i)'s purpose "is to deny protection to websites that tolerate users who flagrantly disrespect copyrights."[47] Still, the court emphasized that, as required by § 512(m), "service providers have no affirmative duty to police their users"[48]:

(m) Protection of privacy.—Nothing in this section shall be construed to condition the applicability of subsections (a) through (d) on —

---

[43] 17 U.S.C. § 512(k)(1)(B).

[44] Capitol Records, Inc. v. MP3tunes, LLC, 821 F. Supp. 2d 627, 637 (S.D.N.Y. 2011) (citing In re Aimster Copyright Litig., 334 F.3d 643, 655 (7th Cir. 2003)).

[45] 17 U.S.C. § 512(i)(1).

[46] Capitol Records, Inc. v. MP3tunes, LLC, 821 F. Supp. 2d 627, 637 (S.D.N.Y. 2011) (citing Perfect 10 v. CCBill, 488 F.3d 1102, 1109-1110 (9th Cir. 2007)).

[47] *Id.* (citing Corbis Corp. v. Amazon.com, 351 F.Supp.2d 1090, 1100-01 (W.D. Wash. 2004)).

[48] *Id.* (citing CCBill, 488 F.3d at 1111).

> **(1)** a service provider monitoring its service or affirmatively seeking facts indicating infringing activity, except to the extent consistent with a standard technical measure complying with the provisions of subsection (i) . . .[49]

Finally, § 512(i)(1)(B)'s specific requirement that the service provider "not interfere with standard technical measures"[50] mandates the accommodating those measures which "have been developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process," among other requirements.[51]

3. Additional Requirements for Safe Harbor under § 512(c)

Beyond the basic threshold requirements, both general VPS and seedbox providers seeking safe harbor protection would need to meet the particular requirements for § 512(c) providers with "[i]nformation residing on systems or networks at [the] direction of users."[52] This kind of service provider must further meet the requirement of properly designating an agent to receive notices of claimed infringement,[53] as well as these more demanding requirements, explained in detail in the following section:

> **(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),[54] responds expeditiously to remove, or disable access

---

[49] 17 U.S.C. § 512(m).

[50] 17 U.S.C. § 512(i)(1)(B).

[51] 17 U.S.C. § 512(i)(2).

[52] 17 U.S.C. § 512(c).

[53] 17 U.S.C. § 512(c)(2).

[54] Copyright holders may send a notice of alleged infringement, meeting particular requirements set in § 512(c)(3), to the designated § 512(c)(2) agent. Upon receiving this notice, as § 512(c)(1)(A)(iii) requires, the provider must "act[] expeditiously to remove, or disable access to, the material."

to, the material that is claimed to be infringing or to be the subject of infringing activity.[55]

B. Section 512(c) Case Law

1. Section 512(c)(1)(A), Knowledge of Infringement

Circuit in *Viacom*[56] and the Ninth Circuit in *UMG Recordings*[57] have clarified that § 512(c)'s knowledge provisions § 512(c)(1)(A)(i) ("actual knowledge") and § 512(c)(1)(A)(ii) ("red flag knowledge") both "refer to knowledge of specific instances of infringement" rather than "general awareness that there are infringements."[58] The Second Circuit reasoned that service providers cannot "expeditiously remove" infringing material, as § 512(c)(1)(A)(iii) requires, if they do not specifically know what infringing material to remove.[59]

The division between the actual and red flag knowledge provisions is significant; that the two provisions both require specific knowledge does not render one of them superfluous.[60] The Second and Ninth Circuits agreed that the actual and red flag knowledge provisions differed simply in imposing subjective versus objective standards.[61] Whereas "the actual knowledge provision turns on whether the provider actually or 'subjectively' knew of specific infringement . . . 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."[62] What exactly constitutes specific knowledge remains largely undefined, although courts have noted that internal emails mentioning specific instances of infringing activity [63] or smoking gun words on a site including "pirate" or "bootleg"[64] could indicate actual or red flag specific knowledge.

---

[55] 17 U.S.C. § 512(c)(1).

[56] Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 31–32 (2d Cir. 2012).

[57] UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022, 1037–38 (9th Cir. 2011).

[58] *See* 17 U.S.C. § 512(c)(1)(A)(i)-(ii).

[59] *Viacom Int'l, Inc.*, 676 F.3d at 30–31 (citing Viacom Int'l, Inc. v. YouTube, 718 F. Supp. 2d 514, 519, 523 (S.D.N.Y. 2010)) (internal quotation marks omitted).

[60] *Id.* at 31.

[61] *Id.* at 31–32 (citing *UMG Recordings, Inc.*, 667 F.3d at 1037–38).

[62] *Id.* at 31.

[63] *See id.* at 33–34 (discussing emails by one of YouTube's founders which pointed to specific knowledge of infringing videos hosted by YouTube).

[64] *See* Capitol Records, Inc. v. MP3tunes, LLC, 821 F. Supp. 2d 627, 644 (S.D.N.Y. 2011) (indicating that particular words could indicate illegal purposes).

For demonstrating actual or red flag knowledge under § 512(c)(1)(A), the Second Circuit has also recently held that common law willful blindness doctrine could "demonstrate knowledge or awareness of specific instances of infringement under the DMCA."[65] Generally, someone would be willfully blind when "aware of a high probability of the fact in dispute and consciously avoid[ing] confirming that fact."[66] But the Second Circuit emphasized that § 512(m), by requiring that service providers need not affirmatively monitor their users,[67] "limits . . . the [applicability of the] doctrine."[68] Although other circuits have yet to discuss the applicability of willful blindness in DMCA safe harbor analysis, courts have commonly understood that "[w]illful blindness is knowledge, in copyright law."[69]

2. § 512(c)(1)(B), Financial Benefit and the Right and Ability to Control

Next in the § 512(c) analysis is the "right and ability to control" requirement in § 512(c)(1)(B), over which the Ninth and Second Circuits once split.[70] The Ninth Circuit had held that, even with "the legal right and necessary technology to remove infringing content . . . until [a provider] becomes aware of specific unauthorized material," it would not have "the kind of ability to control infringing activity [that] the statute contemplates."[71] The Second Circuit found that this interpretation of § 512(c)(1)(B) would make the section duplicative of § 512(c)(1)(A).[72] "Any service provider that has item-specific knowledge of infringing activity and thereby obtains financial benefit would already be excluded from the safe harbor under § 512(c)(1)(A) for having specific knowledge of infringing material and failing to effect expeditious removal."[73] The Second Circuit also rejected an interpretation of the provision that would "codif[y] the common law doctrine of vicarious copyright liability" because it would

---

[65] *Viacom Int'l, Inc.*, 676 F.3d at 35. *See also* UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006, 1023 (9th Cir. 2013) (citing *Viacom Int'l, Inc.*, 676 F.3d at 31) ("a service provider cannot willfully bury its head in the sand to avoid obtaining such specific knowledge").

[66] *Id.* (internal quotation marks omitted).

[67] 17 U.S.C. § 512(m) (2006).

[68] *Viacom Int'l, Inc.*, 676 F.3d at 35.

[69] *Id.* (quoting *In re* Aimster Copyright Litig., 334 F.3d 643, 650 (7th Cir. 2003)).

[70] *See Viacom Int'l, Inc.*, 676 F.3d at 36–37 (contrasting its holding with the *Shelter Capital* case). The Ninth Circuit has recently followed the Second Circuit's interpretation of § 512(c)(1)(B) in its updated UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006, 1027–28 (9th Cir. 2013), opinion.

[71] UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022, 1041 (9th Cir. 2011).

[72] *See Viacom Int'l, Inc.*, 676 F.3d at 36–37.

[73] *Id.* at 36.

create a "catch22."[74] Instead, it chose to "require[] something more than the ability to remove or block access to materials [hosted by] a service provider."[75] What exactly comprises "something more" remains unanswered,[76] but the Second Circuit suggested that inducement as outlined in *Grokster*[77] "might also rise to the level of control under § 512(c)(1)(B)."[78]

Section 512(c)(1)(B) further requires that a service provider not "receive a financial benefit directly attributable to the infringing activity."[79] Courts have found guidance from legislative history emphasizing that, "[i]n general, a service provider conducting a legitimate business would not be considered to receive a financial benefit directly attributable to the infringing activity where the infringer makes the same kind of payment as non-infringing users of the provider's service."[80] The infringing activity must serve as a "draw for subscribers, not just an added benefit."[81] A service provider may still also indirectly financially benefit from the infringing activity of its users, especially if the service provider does not promote infringement.[82]

III. APPLYING DMCA § 512(C) TO VIRTUAL PRIVATE SERVERS

Although case law interpreting § 512(c) continues to evolve, good-faith VPS providers allowing BitTorrent clients should generally be able to find safe harbor protection as long as they strive to be DMCA-compliant.

---

[74] *Viacom Int'l, Inc.*, 676 F.3d at 36–37.

[75] *Id.* at 38.

[76] *See id.* (remanding this "more difficult[] question" to the district court).

[77] Metro–Goldwyn–Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 936–37 (2005). The Supreme Court in *Grokster* explained that "[e]vidence of 'active steps . . . taken to encourage direct infringement'" demonstrates inducement. *Id.* at 936 (internal citation omitted).

[78] *Viacom Int'l, Inc.*, 676 F.3d at 38. The Second Circuit also notes that Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146 (C.D.Cal. 2002), provides an example of a service provider who had the § 512(c)(1)(B) right and ability to control infringing activity. That service provider monitored user websites and required they conform to "detailed instructions." *Perfect 10, Inc.*, 213 F. Supp. 2d at 1173.

[79] 17 U.S.C. § 512(c)(1)(B) (2006).

[80] *See* Capitol Records, Inc. v. MP3tunes, LLC, 821 F. Supp. 2d 627, 645 (S.D.N.Y. 2011) (citing Costar Grp. Inc. v. Loopnet, Inc., 164 F.Supp.2d 688, 704–05 (D. Md. 2001) (quoting H.R.Rep. No. 105-551, Part 2, at 54)).

[81] Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1117 (9th Cir. 2007) (citing Ellison v. Robertson, 357 F.3d 1072, 1078–79 (9th Cir. 2004)).

[82] *See* Capitol Records, Inc. v. MP3tunes, LLC, 821 F. Supp. 2d 627, 645 (S.D.N.Y. 2011).

The DMCA would especially protect general VPS providers, and these providers need not expressly prohibit all BitTorrent use. However, seedbox providers, who expressly target BitTorrent users, would find getting safe harbor protection problematic, particularly if courts strictly apply the Second Circuit's suggested willful blindness doctrine for knowledge or if these providers induce users to engage in copyright infringement.[83]

To qualify for the safe harbor, virtual private server providers must first meet the § 512(k) and § 512(i) threshold requirements, fall under the § 512(c) category's scope, and meet § 512(c)'s specific requirements.

Conscientious seedbox and general VPS providers should have no problem meeting the threshold requirements. VPS providers provide servers for their customers and, thus, are "provider[s] of online services" or "operator[s] of facilities therefor," as required by § 512(k).[84] Furthermore, it is not difficult to maintain a repeat infringer policy as required by § 512(i).[85] Upon receipt of a copyright infringement notice regarding a specific user's account, a general VPS provider could warn that user and ban or restrict the user's account after repeated transgressions. The provider could also make this policy clear whenever a user creates an account. VPS providers expressly marketing themselves as seedbox providers could implement similar policies. It may be likely that they would receive notices more frequently than other virtual private server providers, but as long as they likewise implement a reasonable repeat infringer policy, they should meet the § 512(i) threshold requirement.

Similarly, both general VPS providers and seedbox providers would easily meet the initial qualification for safe harbor under § 512(c). A customer renting either a general VPS or seedbox privately manages the computer space and resources allotted by the provider, who would not place any infringing content on a particular customer's virtual private server. Thus, the relevant potentially infringing material would only exist on the provider's servers "by reason of the storage at the direction of a user."[86] And designating an agent to receive notices, as required by § 512(c)(2), is merely a matter of making a conscientious effort to be DMCA-compliant and choosing somebody.[87]

Neither general VPS providers nor seedbox providers should face a real problem with the actual knowledge requirement as defined by §

---

[83] *Viacom Int'l, Inc.*, 676 F.3d at 35.

[84] *See* 17 U.S.C. § 512(k)(1)(B) (2006).

[85] *See* 17 U.S.C. § 512(i).

[86] 17 U.S.C. § 512(c)(1).

[87] 17 U.S.C. § 512(c)(2).

512(c)(1)(A)(i)[88] and interpreted as knowledge of specific infringement by the Second and Ninth Circuits.[89] VPS providers can only "actually know" of specific instances of infringement by either breaching their clients' privacy expectations or learning from notices received from copyright holders or their representatives. Virtual private servers are, by nature, private, and § 512(m) ensures that providers face no affirmative duty to monitor besides using "standard technical measures."[90]

There is no standard process for server providers to find infringing BitTorrent content on users' private spaces. Server providers that want to preemptively block infringing content typically either prohibit BitTorrent traffic completely,[91] or deal with it on a case-by-case basis.[92] To be able to effectively monitor for infringing content, a provider would have to install fairly complex software on every individual virtual private server—far from a standard technical measure and, instead, much more like sophisticated, unwanted surveillance. The nature of VPS simply prohibits providers from using automated systems for detecting infringing content on their servers as YouTube might do.[93] Whereas YouTube users submit content through the YouTube website, each particular VPS is individually and privately maintained as a separate "virtual machine" with software and other settings chosen by the user.[94] VPS providers may only realistically have actual knowledge of specific infringing content on their servers when copyright holders and their representatives send takedown notices or other complaints.[95] To the extent that a VPS provider may become aware of specific infringing material through § 512(c)(3)-compliant takedown

---

[88] 17 U.S.C. § 512(c)(1)(A)(i).

[89] *See* Viacom Intern., Inc. v. YouTube, Inc., 676 F.3d 19, 31–32 (citing *UMG Recordings, Inc.*, 667 F.3d at 1037–38) (2d Cir. 2012).

[90] 17 U.S.C. § 512(m)(1).

[91] *See, e.g.*, *Terms of Service*, HOSTGATOR, http://www.hostgator.com/tos (last visited Nov. 18, 2012) (prohibiting "bit torrent application[s]" completely).

[92] *See, e.g.*, *Terms of Service*, DOTBLOCK, http://www.dotblock.com/terms.php (last visited Nov. 18, 2012) (stating its policy to "expeditiously remove" unauthorized copyrighted material mentioned in takedown notices).

[93] *See* Timothy B. Lee, *As Curiosity Touches Down on Mars, Video Is Taken Down from YouTube*, ARS TECHNICA (Aug 6, 2012, 6:10 PM), http://arstechnica.com/tech-policy/2012/08/as-curiosity-touches-down-on-mars-video-is-taken-down-from-youtube/ (describing how YouTube's automated content filtering system prevents infringing content from being uploaded and shared with the world, sometimes erroneously).

[94] *See* G.F., *supra* note 12 (describing the separateness of particular virtual private servers and virtual machines more generally).

[95] *See id.*

notices, they must expeditiously remove the infringing material, but, again, this is a matter of conscientiousness.

General VPS providers and seedbox providers alike appear similarly unlikely to have "aware[ness] of facts or circumstances from which infringing activity is apparent."[96] Plaintiffs would likely find it difficult to demonstrate that general virtual private server providers had objective clues about *specific* instances of infringement, as required by statute.[97] In *Capitol Records*, the Southern District of New York required the plaintiffs to have mentioned specific infringing files residing on MP3Tunes's servers in their takedown notices.[98] Similarly, in *Viacom* the Second Circuit did not look beyond infringing videos that high-level YouTube employees had specifically mentioned in internal emails.[99] Again, here, providers would be unlikely to manually peruse customers' files and gain red flag knowledge of specific infringement, regardless of whether they know their customers use BitTorrent on their servers. Certainly, as in *Viacom*, if the providers' directors or employees discussed specific instances of likely infringing material residing on their servers in internal emails, there might be red flag knowledge of specific infringement.[100] But as long as there is no evidence of this kind, courts are unlikely to conclude that there is red flag knowledge. To hold otherwise could endanger the legality of commonly used services like Amazon MP3, iCloud, and Dropbox, which all involve large amounts of infringing material (in addition to non-infringing material) stored by users on remote servers.[101] Courts may be reluctant to put into flux the legality of widely popular services enabled by novel technologies such as cloud computing and storage.[102]

However, seedbox providers, who set up BitTorrent clients for their customers, are more vulnerable to the knowledge provisions if courts strictly interpret willful blindness doctrine, which can, again, "demonstrate knowledge or awareness of specific instances of infringement under the

---

[96] 17 U.S.C. § 512(c)(1)(A)(ii) (2006).

[97] *See* Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 31 (2d Cir.) (explaining that the knowledge provisions apply only to specific instances of infringement).

[98] Capitol Records, Inc. v. MP3tunes, LLC, 821 F. Supp. 2d 627, 642-43 (S.D.N.Y. 2011).

[99] *Viacom Int'l, Inc.*, 676 F.3d at 33–34.

[100] *See id.*

[101] *See generally* Trout, *supra* note 38 (analyzing liability and DMCA safe harbor protection of cloud services, including Dropbox).

[102] *See* Jonathan Zittrain, *A History of Online Gatekeeping*, 19 HARV. J.L. & TECH. 253, 298 (2006) (noting that "judicial activity [] has been appropriately willing to abstain from major intervention in the private development of information technology").

DMCA."[103] Plaintiffs might argue that seedbox providers are aware of a high probability of their customers using BitTorrent on their servers to download and upload infringing material, especially if they market themselves as providing "seedboxes." A substantial portion of BitTorrent use is likely to be infringing.[104] So if all of a provider's customers operate BitTorrent clients through their servers, a provider may know that there is at least a high probability that much of the data stored is infringing. With this knowledge of a high probability of infringement, a service provider consciously setting up servers that are private, in order to avoid confirming knowledge of infringement might be willfully blind.[105]

The non-infringing uses of BitTorrent remain noteworthy,[106] but seedbox providers might know that there are great incentives for users mostly interested in infringement to rent a seedbox.[107] Still, courts have interpreted "knowledge" as regarding *specific* instances of infringement.[108] Perhaps plaintiffs must then show that providers are willfully blind to specific instances of infringement—potentially difficult unless copyright holders have repeatedly issued § 512(c)(3)-compliant takedown notices that were ignored by providers. General VPS providers are not particularly vulnerable, but if seedbox providers receive numerous takedown notices, they may find it difficult to show they were not willfully blind—that they were not consciously avoiding confirming a fact of infringement. Although the application of this common law doctrine to § 512(c)'s knowledge requirements remains somewhat unclear,[109] courts may be hesitant to grant safe harbor protection to meticulous but suspicious seedbox providers.

---

[103] *See Viacom Int'l, Inc.*, 676 F.3d at 34-35.

[104] *See* Jacqui Cheng, *BitTorrent Census: About 99% of Files Copyright Infringing*, ARS TECHNICA (Jan 29, 2010, 2:08 PM), http://arstechnica.com/business /2010/01/bittorrent-census-about-99-of-files-copyright-infringing/ (describing a study that found that the vast majority of files shared through BitTorrent were infringing).

[105] *See Viacom Int'l, Inc.*, 676 F.3d at 35 (setting a two-prong willful blindness standard in the DMCA safe harbor context).

[106] *See* Helton, *supra* note 16 at 2 (providing notable examples of non-infringing BitTorrent use by film maker Peter Jackson and the National Aeronautics and Space Administration); Bangeman, *supra* note 4 (providing notable examples of non-infringing uses of BitTorrent by established video game developers Blizzard Entertainment and Valve Corporation).

[107] *See 10 Reasons Why You Need a Seedbox*, *supra* note 21.

[108] *Viacom Int'l, Inc.*, 676 F.3d at 30.

[109] *See Viacom Int'l, Inc.*, 676 F.3d at 34 (describing, as recently as 2012, willful blindness's applicability to DMCA safe harbor as an "issue of first impression" in the Second Circuit).

Even if general VPS providers or seedbox providers do not have § 512(c)(1)(A) knowledge, they would still lose § 512(c) safe harbor protection if they receive a direct financial benefit from infringing activity while having the right and ability to control the infringing activity.[110] Seedbox providers will face greater difficulty than general VPS providers in meeting this requirement.[111] Regarding the "right and ability to control," VPS providers do not generally exert specific control over each particular act of infringing or non-infringing filesharing (as required by the Ninth Circuit).[112] But some, especially seedbox providers, assist users with setting up BitTorrent clients on their virtual private servers—arguably, an "affirmative step[] taken to foster infringement" that could constitute inducement as defined by *Grokster*.[113] Although "ordinary acts incident to product distribution, such as offering customers technical support . . . [would not] support liability in themselves,"[114] seedbox providers could imaginably reach out to BitTorrent communities and look for customers who want to upload and download infringing content. Courts have not yet decided what exactly constitutes the required level of control,[115] but seedbox providers are likely to face these sorts of problems in securing DMCA safe harbor protection.

Nevertheless, general VPS providers, at least, are unlikely to receive a financial benefit directly attributable to the infringing activity; infringing activity should not specifically serve as a special "draw" for subscribing users.[116] General VPS providers provide servers usable for a wide variety of purposes, many of which are wholly unrelated to copyright infringement. These providers charge different rates for more space, more

---

[110] *See* 17 U.S.C. § 512(c)(1)(B) (2006).

[111] *See* 17 U.S.C. § 512(c)(1)(A)(iii) (2006).

[112] *See* UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022, 1041 (9th Cir. 2011) (explaining that, "until [a service provider] becomes aware of specific unauthorized material, it . . . does not have the kind of ability to control infringing activity the statute contemplates").

[113] *See* Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 936-37 (2005).

[114] *Id.*

[115] *See Viacom Int'l, Inc.*, 676 F.3d at 38.

[116] Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1117 (9th Cir. 2007) (citing Ellison v. Robertson, 357 F.3d 1072, 1078–79 (9th Cir. 2004)). The *Perfect 10* court also cited legislative history when explaining that "receiving a one-time set-up fee and flat, periodic payments for service from a person engaging in infringing activities would not constitute receiving a 'financial benefit directly attributable to the infringing activity.'" *Id.* (citation omitted).

bandwidth, and more processing power,[117] independent of whether a customer wants to upload and download unauthorized copyrighted works. Because the "value of the service" for a general VPS provider does not "lie[] in providing access to infringing material,"[118] courts should not find that infringing activity on those services serve as a special "draw" for subscribing users.

Seedbox providers similarly sell their services independent of whether customers are engaged in copyright infringement. However, plaintiffs might argue that, because seedboxes enable convenient BitTorrent use, and BitTorrent is overwhelmingly used for copyright infringement, seedbox providers directly profit from infringing activity by drawing subscribers specifically for infringement. Thus, courts may find that seedbox providers, operating only BitTorrent-related virtual private servers, derive direct financial benefit from infringing activity. In contrast, as long as general VPS providers refrain from charging customers varying rates, courts are unlikely to find that they "directly benefit from . . . their user's infringing activity."[119]

CONCLUSION

As more BitTorrent users seeking infringing material operate BitTorrent remotely instead of using home connections, the question of copyright infringement liability of both "general" virtual private server providers and seedbox providers, who market expressly to BitTorrent users, becomes particularly pertinent. And as the recording and film industries continue waging a war against infringing filesharing,[120] they may soon sue providers who allow potentially large-scale infringing use of BitTorrent to continue on their servers. The Digital Millennium Copyright Act's safe harbor provisions offer potential protection to both kinds of VPS providers from liability for customers' infringing files.[121] However, seedbox providers

---

[117] *See, e.g.*, *Virtual Private Server*, OVH.CO.UK, http://www.ovh.co.uk/vps/ (last visited Nov. 18, 2012); *Why an EvoBoxes Virtual Server?*, EVOBOXES, https://evoboxes.org/vps.php (last visited Nov. 18, 2012); *Pricing & Signup*, DOTBLOCK, https://billing.dotblock.com/order (last visited Nov. 18, 2012); LINODE.COM, http://www.linode.com (last visited Nov. 18, 2012).

[118] *See Ellison*, 357 F.3d at 1079 ("the central question of the 'direct financial benefit' inquiry in this case is whether the infringing activity constitutes as a draw for subscribers, *not just an added benefit*" (emphasis added)).

[119] *See Capitol Records, Inc.*, 821 F.Supp. 2d at 645 (citing Costar Grp. Inc. v. Loopnet, Inc., 164 F.Supp.2d 688, 704-05 (D. Md. 2001) (quoting H.R.Rep. No. 105-551, Part 2, at 54)).

[120] *See* Kravets, *supra* note 18; Lindenberger, *supra* note 18.

[121] *See* 17 U.S.C. § 512(c) (2006).

may find it difficult to gain safe harbor protection. They might consciously avoid knowledge of infringement and, thus, be willfully blind to knowledge of infringement, and they may be directly benefitting from infringement, while potentially encouraging infringing activity. In contrast, conscientious general VPS providers with customers operating BitTorrent on their servers are likely to receive DMCA safe harbor protection.

It is important that the DMCA protect general VPS providers. Without protection from liability for content stored by customers, virtual private server providers and potentially, by extension, cloud service providers would be unlikely to survive the specter of copyright litigation. Good-faith technological entrepreneurs should be able to innovate and drive America's economy forward, while bad-faith actors should not be able to free-ride at the expense of copyright owners. Deciding that the societal benefits of these valuable innovations would outweigh the costs of potential infringement, a prescient Congress attempted to strike this balance by creating DMCA safe harbor protection. Accordingly, although seedbox providers may not escape liability through the safe harbor provisions, the safe harbor provisions' balancing act should rightly protect good-faith technological services like general virtual private servers.