

TULANE JOURNAL OF TECHNOLOGY AND INTELLECTUAL PROPERTY

VOLUME 15

FALL 2012

A Good Idea at the Time: Recent Digital Millennium Copyright Act § 512(c) Safe Harbor Jurisprudence—Analysis and Critique of Current Applications and Implications

Martin B. Robins*

I.	INTRODUCTION	2
II.	BACKGROUND AND RATIONALE	3
III.	CURRENT CONSIDERATIONS	3
IV.	STATUTORY FOUNDATION	6
	A. <i>Who Is a “Service Provider”?</i>	6
	B. <i>Other Provisions</i>	8
V.	EFFORTS OF THE COURTS	10
	A. <i>Veoh</i>	10
	B. <i>YouTube</i>	14
	C. <i>Grokster</i>	17
VI.	CASE LAW OVERVIEW	19
VII.	APPLICATION OF THE CASE LAW	20
VIII.	SITE MONITORING? BANE OR BOON, AND FOR WHOM?	22
IX.	A TECHNOLOGICAL ALTERNATIVE.....	23

* © 2012 Martin B. Robins. Mr. Robins is a partner with the Chicago office of the Atlanta-based law firm of Fisher Broyles LLP with a corporate transactional practice emphasizing technology and intellectual property matters, as well as an adjunct professor at DePaul University College of Law. He has also been an adjunct professor at Northwestern University School of Law. He holds a Bachelor of Science degree in economics (summa cum laude) from the Wharton School of the University of Pennsylvania and a Juris Doctor degree (cum laude) from Harvard Law School. Comments are eagerly solicited and should be directed to mrobins@fisherbroyles.com. The views expressed in this article are solely those of the author and do not necessarily represent those of Fisher Broyles LLP. The author wishes to acknowledge the invaluable input of Alan Wernick, Esq., also a partner with Fisher Broyles LLP.

X.	REVISITING WHO IS A SERVICE PROVIDER: AN INVITATION TO ARGUMENTATION AND LEGISLATION.....	26
XI.	CONCLUSION	29

I. INTRODUCTION

In a rare fit of prescience and technical acumen, the United States Congress in 1998 enacted the Digital Millennium Copyright Act (DMCA).¹ In pertinent part, the legislative history indicates that this statute, specifically Title II, was intended to facilitate the growth of the then-nascent Internet and World Wide Web by immunizing from vicarious liability for copyright infringement by third parties, those who provided public access to the Internet.² Absent such immunity, under traditional principles of copyright law, such providers of the technical infrastructure might well have been liable for any infringing material that they carried, even if it appeared on their network as a result of the actions of a member of the public unknown to them—an obvious impediment to development of and reasonable pricing for the mechanisms needed for widespread access.³

As one court elaborated:

Although Congress was aware that the services provided by companies like [defendant] are capable of being misused to facilitate copyright infringement, it was loath to permit the specter of liability to chill innovation that could also serve substantial socially beneficial functions.

1. Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended in scattered sections of 17 U.S.C.).

2. While the DMCA addresses numerous matters pertaining to creation and transmission of electronic (“digital”) material, this article focuses on the so-called “service provider safe harbor” contained in DMCA § 512(c), which immunizes (at the least) internet portal companies from liability for infringing transmissions of their customers where the portal company had no control over the material that was carried. “Difficult and controversial questions of copyright liability in the online world prompted Congress to enact Title II of the DMCA, the Online Copyright Infringement Liability Limitation Act (OCILLA).” *Ellison v. Robertson*, 357 F.3d 1072, 1076 (9th Cir. 2004) (citation omitted). Congress recognized, “[I]n the ordinary course of their operations service providers must engage in all kinds of acts that expose them to potential copyright infringement liability.” S. REP. No. 105-190, at 8 (1998). “To that end, OCILLA created four safe harbors that preclude imposing monetary liability on service providers for copyright infringement that occurs as a result of specified activities.” *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 667 F.3d 1022, 1030 (9th Cir. 2011).

3. *See generally* 17 U.S.C. §§ 101, 501 (describing subject matter and infringement of copyright, respectively). While the so-called “fair use” defense contained in 17 U.S.C. § 107 (the “regular” Copyright Act) and well described in *Wall Data Inc. v. L.A. Cnty. Sheriff’s Dep’t*, 447 F.3d 769 (9th Cir. 2006), is often relied upon in infringement cases where someone has reproduced someone else’s copyrighted material, by its terms, this defense is rarely, if ever, available to a service provider.

Congress decided that “by limiting [service providers’] liability,” it would “ensure[] that the efficiency of the Internet will continue to improve and that the variety and quality of services on the Internet will continue to expand.”⁴

This approach made great sense in 1998 and even today contains the foundation for sensible regulation. However, unforeseeable changes in technology and practice, as well as what the author considers to be some curious strategic decisions by litigants and outcomes in the relatively few litigation matters which have addressed this topic, militate in favor of several changes and clarifications in this regimen.

II. BACKGROUND AND RATIONALE

Recognizing the immense social and commercial significance of the Internet, Congress correctly determined that private investment would flow only if providers could safely carry customer traffic without having to vet such traffic for compliance with copyright laws. In response, Congress included in the final DMCA § 512, which contains several provisions to this effect.⁵ Most notable are subsections (a) and (c), which provide several “safe harbors” from liability for customer infringement for those who qualify as “service providers” as defined and in general do not edit or otherwise alter the content, do not have a direct financial interest in its transmission, and satisfy certain procedural requirements, discussed *infra*.⁶

III. CURRENT CONSIDERATIONS

As one recent commentator on this topic has noted:

At the time that Congress crafted this regime, the World Wide Web was a simpler place. OSPs [online service providers] hosted websites managed by webmasters who actively controlled the materials made available on

4. *UMG Recordings*, 667 F.3d at 1030 (alterations in original) (quoting S. REP. No. 105-190, at 8 (1998)).

5. 17 U.S.C. § 512 (2006).

6. 17 U.S.C. § 512(a) and (c) are also known as and hereinafter referenced as the OCILLA—Online Copyright Infringement Liability Limitation Act. In *Viacom International Inc. v. YouTube, Inc.*, 676 F.3d 19, 27 (2d Cir. 2012), which is discussed in detail *infra* notes 51—77 and accompanying text, the key statutory provisions are 17 U.S.C. § 512(a), § 512(c), § 512(i), § 512(k), § 512(m), and § 512(n).

Subsection (k) actually contains two definitions of a service provider. See discussion *infra* note 15 and accompanying text.

webpages. Industry negotiators had a relatively clear sense of how the safe harbor would function in this Web 1.0 ecosystem.⁷

As technology evolved to allow easy submission and posting to Web sites of user-generated content from computers, MP3 devices, smartphones, digital cameras, webcams, and the like, none of which existed in any commercially meaningful sense when the DMCA was enacted, this provision has taken on greater significance.⁸

Probably the most fundamental change in the web over the last 10 years has been the rise of “user generated content,” that is, the shift from websites that present packaged content created or controlled by the website owner, to websites that are essentially services for publishing content uploaded by others.⁹

With this significance has come legal uncertainty:

The emergence of Web 2.0 applications, such as UGC [user-generated content] sites, in 2004, complicated application of this regime in not fully anticipated ways. With users gaining the ability to upload, edit, and collaborate in information dissemination, webmasters came to be replaced by automated systems and the potential liability of OSPs became more uncertain.¹⁰

Along with, and probably in large part because of, the development and widespread adoption of easy-to-use hardware, came Web sites which either existed solely to accommodate user-generated content or strongly encouraged its submission as part of a promotional strategy.¹¹

Many Web site operators in this space rely heavily upon the terms of this safe harbor as a foundation of their business model. The author, in his practice, has observed numerous firms with major interactive Web presences, who are not only cognizant of the provision’s terms, but make every effort to comply with its letter and spirit as a fundamental part of

7. Peter S. Menell, *Judicial Regulation of Digital Copyright Windfalls: Making Interpretive and Policy Sense of Viacom v. YouTube and UMG Recordings v. Shelter Capital Partners*, MEDIA INST. (May 3, 2012), <http://www.mediainstitute.org/IPI/2012/050212.php>.

8. See Stephen M. Kramarsky, *How Safe is the DMCA ‘Safe Harbor’ after ‘Viacom v. YouTube’?*, N.Y.L.J., May 15, 2012, at 5, available at <http://www.newyorklawjournal.com/PubArticleNY.jsp?id=1202553482917&slreturn=120120910172728>.

9. *Id.*

10. Menell, *supra* note 7.

11. YouTube, Twitter, Facebook, and LinkedIn are examples of the former, while examples of the latter are found at numerous sites marketing consumer products, which encourage consumers to post comments and videos reflecting their experience with products such as cookies, cars, and sports equipment. For example, on its Web site, SportsNation, the fan forum and poll section of ESPN.com, invites site visitors to “Submit a Link” and then uses the videos and web information gathered as a majority of the material later aired on the daily television show. ESPN SPORTSNATION, <http://espn.go.com/sportsnation/> (last visited Oct. 26, 2010).

their risk management effort. There can be no doubt as to its commercial significance. For example, Google reports that it receives 350,000 takedown notices each week.¹²

All would agree that several tsunamis of infringing textual, audio, and video material are posted to such sites every day. While legal claims may be brought (and have been successfully brought) against the actual infringers, for the most part, this is not a practical alternative.¹³ It is often difficult to locate them, and they are frequently judgment-proof. For copyright holders, it is much more efficient to sue intermediary firms operating Web sites, who, in some sense, provide the means of infringement to large numbers of persons.

A key issue for further growth of the Internet is the extent to which the safe harbor requires the operators of Web sites that are used for such purposes to take action to mitigate the extent of infringement.¹⁴ This Article examines and critiques the sparse early jurisprudence under the safe harbor as it impacts both current practice and future jurisprudence, and suggests certain steps that should be considered by market participants and counsel addressing these situations from the standpoint of Web site operations or exploitation of digital copyrighted content.¹⁵

12. See Kevin Collier, *Google Hit with a Staggering 350,000 DMCA Takedown Requests Every Week*, DAILY DOT (May 28, 2012), <http://www.dailydot.com/news/dmca-takedown-request-google-microsoft/> (suggesting that Microsoft sent over 94,000 takedown requests during the week beginning May 21, 2012); *infra* text accompanying note 31.

13. See, e.g., Ben Sheffner, *Tenenbaum Takes the Stand*, ARS TECHNICA (July 30, 2009, 5:30 PM), <http://arstechnica.com/tech-policy/2009/07/tenenbaum-takes-the-stand-i-used-p2p-and-lied-about-it> (elaborating on some successful primary infringement claims).

14. The term “operator” is not a defined term under the statute, which to the author causes unnecessary and undesirable ambiguity. See 17 U.S.C. § 512(k) (2006) (*Definitions*). Discussion and adjudication lump together those who provide access to the web, those who “host”—that is, provide computer facilities which exhibit the content to those who seek it—Web sites for others but do not influence the content of such sites, and those who commission and specify the design and functionality of Web sites. From the “service provider” definition, it is clear to the author and most commentators that Congress intended to immunize at least Internet access providers, and probably web hosts, from liability for third-party infringement. *Cf. id.* (defining “service provider”). It is not as clear that such intention extended to anyone operating a Web site.

15. As noted, even Judge Cabranes in his *YouTube* opinion laments the paucity of guidance. See 676 F.3d 19 (2d Cir. 2012). In the opinion of the author, the two cases emphasized herein will provide the bulk of the guidance that is on point for the foreseeable future, at least until other circuits or the U.S. Supreme Court address the topic in the appropriate context.

IV. STATUTORY FOUNDATION

A. *Who Is a “Service Provider”?*

The safe harbor statute contains many operative provisions, which are discussed *seriatim*, but perhaps none as fundamental as the definition of the term “service provider.” Only those who fall into this category are entitled to the protection offered within the safe harbor. The language of this provision—“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;” and in an alternative provision, “a provider of online services or network access, or the operator of facilities therefor”¹⁶—clearly covers traditional commercial fixed and mobile Internet service providers such as Comcast, Verizon, and AT&T, to name just a few. The first definition is generally understood to apply only to Internet service providers and similar firms and is usually of little relevance in this context. It is the second branch of the clause that is typically at issue.

Whether it covers others who maintain Web sites inviting public submissions seems much less clear to the author. It is far from intuitive that YouTube or Facebook-style entities or firms, which simply allow or encourage public submissions, are engaged in the “transmission, routing, or providing of connections for digital online communications.”¹⁷ However, the courts which have considered the issue have not been as troubled as the author.

In a prominent recent case involving the video-sharing service Veoh Networks, Inc. (Veoh), Judge Fisher of the United States Court of Appeals for the Ninth Circuit described the Web-based company as one that

allows people to share video content over the Internet. Users can view videos uploaded by other users as well as authorized “partner content” made available by major copyright holders such as SonyBMG, ABC and ESPN. There are two ways to use Veoh’s service: through a standalone software client application launched in late 2005, or through the veoh.com website launched in early 2006 that users access via a standard web browser. Both services are provided free of charge. Veoh generates revenue from advertising displayed along with the videos.¹⁸

16. 17 U.S.C. § 512(k)(1).

17. *Id.*

18. *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 667 F.3d 1022, 1026-27 (9th Cir. 2011).

The question of service provider status was taken as a given, and neither discussed in the opinion, nor argued by the plaintiff. Perhaps significantly, Judge Fisher included a footnote making clear that the court was refraining from directly ruling on the issue: “We assume without deciding that Veoh qualifies as a ‘service provider’ because UMG does not contend otherwise.”¹⁹ The topic was indirectly addressed elsewhere in the opinion:

Finally, if Congress wanted to confine § 512(c) exclusively to web hosts rather than reach a wider range of service providers, we very much doubt it would have done so with the oblique “by reason of storage” language. We presume that Congress instead would have taken the more straightforward course of clarifying in the definition of “service provider” that, as it applies to § 512(c), only web hosts qualify.²⁰

However, even this effort begs the question of whether someone who operates—as opposed to hosts—a Web site accepting public submissions is a service provider within the meaning of the statute. The aforementioned footnote reserving the point only adds to the mystery of what the court actually held.

In a more recent (by one year) and much more renowned case involving the well-known YouTube service, Judge Cabranes of the United States Court of Appeals for the Second Circuit paid only slightly more attention to the matter when determining that YouTube is a “service provider”: “First, the party must in fact be a ‘service provider,’ defined, in pertinent part, as ‘a provider of online services or network access, or the operator of facilities therefor.’”²¹ As will be discussed *infra*, the author does not fully subscribe to this conclusory approach, but it does appear to be accepted by courts and litigants.²² This means that at present, at least in the Second and Ninth Circuits, anyone offering Internet access or operating a Web site accepting public submissions should be able to utilize the safe harbor if they satisfy its operative provisions.²³

19. *Id.* at 1030 n.4.

20. *Id.* at 1034.

21. *Viacom Int’l Inc. v. YouTube, Inc.*, 676 F.3d 19, 27 (2d Cir. 2012) (citing 17 U.S.C. § 512(k)(1)(B)). This outcome was subsequently relied upon by the District Court for the Southern District of New York, when it determined in a safe harbor case, “Because the defendant operates a website that permits users to post and share materials, it falls within the broad definition of a service provider under section 512(k)(1)(B).” *Obodai v. Demand Media, Inc.*, No. 11 Civ. 2503 (PKC), 2012 WL 2189-740 (S.D.N.Y. June 13, 2012).

22. *See infra* Part X.

23. The United States Court of Appeals for the Seventh Circuit should be included as well in view of *In re Aimster Copyright Litigation*, 252 F. Supp. 2d 634, 658 (N.D. Ill. 2002), *aff’d*, 334 F.3d 643 (7th Cir. 2003), in which the district court stated: “A plain reading of [17 U.S.C. § 512(k)] reveals that ‘service provider’ is defined so broadly that we have trouble imagining the

A few other courts have also come to such conclusions, in situations not involving sites soliciting public submissions of the same nature as those at issue in *UMG Recordings* and *YouTube*.²⁴ These results seem curious in view of the fact that, in 1998, interactive Web capability was largely theoretical, and little hardware or software existed to make it a reality, let alone commercially relevant. Absent large amounts of bandwidth, it is a frustrating experience at best to view, hear, or submit posts of music, movies, or any animated content; yet, in 1998, dial-up access was the rule. Similarly, a great deal of user-generated content is currently posted via smartphones with built-in video camera capability, but such devices were then unknown. How could Congress have sought to permit the results of technology that did not yet exist in any meaningful sense and was not generally envisioned?

The author suggests, *infra*, that the topic be considered in greater detail in other circuits by both the bench and the bar, and ultimately clarified by Congress.²⁵ One factor that must be given credence is that, appropriately or not, it appears that there is a common understanding, including among counsel with substantial intellectual property and DMCA experience, that the provision is available to anyone operating a Web site. A contrary holding in court or action by Congress may cause at least temporary marketplace disruption. An expansion of the statutory language to conform to current usage and understanding may be called for.

B. Other Provisions

These operative provisions are somewhat involved, and compliance is far from a given. Before the operative provisions come into play, it must be established that the user-generated material is at issue “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.”²⁶ As noted *infra*, this requirement appears to be a focal point for litigation in this area.²⁷

The operative provisions may be summarized as follows:

existence of an online service that *would not* fall under the definitions” The author does not agree that the meaning is so “plain.”

24. See, e.g., *Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090 (W.D. Wash. 2004) (holding that Amazon meets DMCA definition of service provider); *Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082, 1088 (C.D. Cal. 2001) (holding that eBay “clearly” falls within the broad definition of a service provider).

25. See discussion *infra* Part X.

26. 17 U.S.C. § 512(c)(1).

27. See *infra* notes 37-42 and accompanying text.

- The safe harbor claimant must not have “actual knowledge” of infringement in a specific case;²⁸
- The claimant must not receive a financial benefit from the infringing activity;²⁹
- The claimant must not edit or otherwise control the content of the material submitted by the public;³⁰
- The claimant must advise site users and the Copyright Office in writing of the appropriate contact (“agent”) to receive notice from copyright holders of claimed infringement (a “takedown notice”);³¹
- The claimant must promptly remove material which is the subject of such notice;³² and
- The claimant must post on the site, a notice indicating that it will terminate the access of “repeat infringers” and comply with such policy.³³

Interestingly, the provision expressly disclaims any obligation to “monitor” the site to affirmatively identify infringing material before it is the subject of a takedown notice.³⁴ While the procedural steps contained in the safe harbor—e.g., agent designation, repeat infringer policy, and response to takedown notices—are not especially daunting, the other requirements have bedeviled the few courts that have addressed them and

28. See 17 U.S.C. § 512(c)(1)(a)(i). As noted *infra* note 46 and accompanying text, the question of the impact of general knowledge of infringement versus actual knowledge of specific infringement is a key issue in current litigation under the safe harbor provision.

29. See 17 U.S.C. § 512(c)(1)(B). The meaning of this term in practice is open to question. Even without a direct financial benefit from a particular post, one offers Internet access for a fee and solicits public posts in order to sell advertising and/or promote a product. YouTube is claiming the benefits of the safe harbor, notwithstanding the fact it was sold to Google for nearly \$2 billion. See *Viacom Int’l Inc. v. YouTube, Inc.*, 676 F.3d 19, 28 (2d Cir. 2012).

30. See 17 U.S.C. § 512(a), (k)(1)(A).

31. See *id.* § 512(c)(2).

32. See *id.* § 512(c)(1)(C). A service provider is liable for such material not removed, unless it receives a “counter notification” from the person who made the post, see *id.* § 512(g)(3), in which case the required response is unclear from the statute and often unsatisfactory in practice, as indicated by this anecdote involving a person falsely accused of infringement on account of their posting of a birdsong video: *YouTube Birdsong Goof Shows Copyright Problems*, DAILY DOT (Feb. 27, 2012), <http://www.dailydot.com/business/eeplox-rumblefish-youtube-birdsong-copyright/>.

33. See 17 U.S.C. § 512(i)(1)(A). One wonders how claimants who are not traditional internet service providers will comply with such policy; how are they able to bar someone from visiting their site?

34. See *id.* § 512(m). Apart from the requirements of the DMCA, monitoring may be advisable (and is usually done) in order to screen out material that may subject the site operator to liability on account of the material’s being obscene, libelous, or an incitement to violence. Query whether people performing such monitoring is permitted, required, or prohibited from addressing any infringement that they encounter.

led to considerable uncertainty as to the day-to-day meaning of the statute.

V. EFFORTS OF THE COURTS

A. Veoh

The first notable case in this area is *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, which also involved Veoh, an Internet television company similar to the popular YouTube video-sharing service.³⁵ A company holding a large number of copyright registrations brought the suit and alleged that the posting of the registered material on the Veoh site without a license was an infringement of its rights³⁶ and was not protected by the safe harbor for two reasons of interest here: first, Veoh did not satisfy the threshold criterion that the copyrighted material was on its site “by reason of the storage at the direction of a user,” and second, Veoh did have the requisite “actual knowledge” of infringement.³⁷ The Ninth Circuit addressed the matter in the context of the district court’s grant of summary judgment to defendants.³⁸

As to the first point, the plaintiff argued that the work done by Veoh to prepare a user-generated video for placement on the site made the posting effectively Veoh’s (thereby causing it to run afoul of the “by reason of the storage” threshold requirement for the affirmative defense) as opposed to it being merely an intermediary for material submitted by its users.³⁹ However, in the opinion of the author and the court, the plaintiff undermined whatever logical appeal this argument had by heavily relying upon a tortured analogy to the federal Racketeer Influenced and Corrupt Organizations statute (RICO), which contains similar “by reason of” terminology.⁴⁰

While the language similarity is apparent, the RICO statute has nothing whatsoever to do with copyright law and was enacted for a completely different purpose—protection of citizens from violent crime

35. See 667 F.3d 1022, 1026 (9th Cir. 2011).

36. See *supra* note 13 and accompanying text.

37. See *UMG Recordings*, 667 F.3d at 1030-31 (citing 17 U.S.C. § 512(c)(1)). A third major concern for the court was the liability of investors in the Veoh service for its alleged copyright infringements. *Id.* at 45-47. While this is an important commercial concern, it is not pertinent to the underlying substantive analysis.

38. See *id.* at 1029-45.

39. “Facilitation of access, UMG argues, goes beyond ‘storage.’ Therefore the creation of chunked and Flash files and the streaming and downloading of videos fall outside § 512(c). UMG also contends that these automatic processes are not undertaken ‘at the direction of the user.’” *Id.* at 1031.

40. *Id.* (citing 18 U.S.C. §§ 1961-68).

prompted by organized criminal organizations—without Congress giving any indication that it intended the statutes to be read together, such that there is no reason to apply it in this context.⁴¹ As a result, the court had little difficulty holding that the “by reason of” language should be broadly construed: “We hold that the language and structure of the statute, as well as the legislative intent that motivated its enactment, clarify that § 512(c) encompasses the access-facilitating processes that automatically occur when a user uploads a video to Veoh.”⁴² The court made clear that this reading means that the statute may be utilized by anyone operating a Web site instead of only by the party who is actually “hosting” it by placing the content on its servers to permit public access.⁴³ “We do not find persuasive UMG’s effort to reconcile the internal contradictions its reading of the statute creates by positing that Congress must have meant § 512(c) to protect only ‘web hosting’ services. Web hosts ‘host’ websites on their servers, thereby ‘mak[ing] storage resources available to website operators.’”⁴⁴ This broad reading of the threshold requirement substantially expands the value of the safe harbor by allowing its use by a wide range of parties who accept, and even solicit, public submissions. Conversely, this decision makes it considerably harder for copyright holders to prevent infringement, at least using today’s conventional means.⁴⁵

One wonders if an argument by another plaintiff, based upon the specific technical circumstances of the posting of the material at issue, its handling by defendants, and how it is truly attributable to the defendant, might fare better than this plaintiff’s argument based upon the RICO statute. At a minimum, there is significant room for discussion about the precise meaning of the threshold language.

The court also considered at length the issue of whether the inevitability of the posting of some infringing material was sufficient to satisfy the “actual knowledge of infringement” standard of the statute or whether this standard requires knowledge of infringement in specific cases:

41. “None of these concerns applies to the DMCA, which, unlike the Clayton Act and RICO, involves a narrow affirmative defense rather than the expansion of liability. Further, . . . there is no indication that Congress modeled the DMCA on the Clayton Act or RICO.” *Id.* at 1033.

42. *Id.* at 1031.

43. *See id.* at 1034.

44. *Id.* However, the inclusion of footnote 4 in the court’s opinion, discussed *supra* note 19 and accompanying text, in which the court expressly disclaims any decision as to who qualifies as a service provider, is arguably inconsistent with this conclusion.

45. *See infra* note 100 and accompanying text for discussion of possible benefits for copyright holders from use of “digital fingerprints.”

Nevertheless, UMG contends that Veoh hosted a category of copyrightable content—music—for which it had no license from any major music company. UMG argues Veoh thus must have known this content was unauthorized, given its *general knowledge that its services could be used to post infringing material*. UMG urges us to hold that this sufficiently demonstrates knowledge of infringement. We cannot, for several reasons

. . . .
Requiring *specific knowledge* of particular infringing activity makes good sense in the context of the DMCA, which Congress enacted to foster cooperation among copyright holders and service providers in dealing with infringement on the Internet. *See* S. Rep. No. 105-190, at 20 (noting OCILLA was intended to provide “strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements”)⁴⁶

The court reasoned that the legislative purpose for the safe harbor—the facilitation of the use of the Internet for the dissemination of entertainment material—would not be well served by a general knowledge standard, and that such a narrow reading of the statute would render the safe harbor a dead letter when it was obviously intended to have a material impact on apportionment of infringement risk.⁴⁷

While it was not cited in the court’s opinion, it is also logical to believe that the United States Supreme Court’s fairly narrow approach in 2005 to contributory or secondary copyright infringement in the *Grokster* case—in which it required the plaintiff to produce some sort of evidence of the defendant’s intent, as well as evidence that the device at issue had no meaningful noninfringing use—was pertinent to the court.⁴⁸ The Supreme Court sharply distinguished devices such as video recorders which had significant legitimate uses (i.e., time-shifting of programming), from devices such as the *Grokster* peer-to-peer file sharing software, the legitimate uses of which were much less significant than infringing uses and not emphasized by defendants.⁴⁹

The Ninth Circuit placed great emphasis on the notice and takedown provisions of the statute, which put on the copyright holder the

46. *UMG Recordings*, 667 F.3d at 1036-37 (emphasis added).

47. “Further, Congress’ express intention that the DMCA ‘facilitate making available quickly and conveniently via the Internet . . . movies, music, software, and literary works’—precisely the service Veoh provides—makes us skeptical that UMG’s narrow interpretation of § 512(c) is plausible.” *Id.* at 1036 (citing S. REP. No. 105-190, at 8).

48. *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005); see *infra* notes 75-81 and accompanying text.

49. “MGM’s evidence gives reason to think that the vast majority of users’ downloads are acts of infringement” *Metro Goldwyn-Mayer*, 545 U.S. at 923.

burden of demanding that the service provider remove specific infringing material, but then shifts to the provider the onus of removing the offending content from its site: “These considerations are reflected in Congress’ decision to enact a notice and takedown protocol encouraging copyright holders to identify specific infringing material to service providers.”⁵⁰

The court was seemingly quite troubled by the plaintiff’s failure to avail itself of this procedure, which the court considered the “most powerful” tool available to copyright holders, and apparently felt that this alone was largely sufficient to defeat the plaintiff’s claim:

It is undisputed that, until the filing of this lawsuit, UMG “had not identified to Veoh any specific infringing video available on Veoh’s system.” UMG’s decision to forgo the DMCA notice protocol “stripped it of the most powerful evidence of a service provider’s knowledge—actual notice of infringement from the copyright holder.”⁵¹

While the court is correct that this procedure is important and should be used by copyright holders, it is somewhat surprising that the court treats the notice and takedown provision as an apparent condition precedent to maintenance of an infringement suit when it does not appear from the language of the statute that Congress intended for this to be the case. Analogizing from the physical world to the digital one, while courts generally tend to look favorably upon efforts to resolve infringement (and usually other IP-based) disputes through discussions among the parties prior to resorting to litigation, there is no such firm requirement.⁵² It is surprising that one is being introduced here.

The significance of the Ninth Circuit’s reasoning must be acknowledged. It clearly stands for an expansive, pro-site operator view of the safe harbor that complicates the efforts of copyright holders to protect their rights. However, it also appears to raise—for both parties—the stakes associated with the notice and takedown process. It would appear that, at least in the Ninth Circuit, if a copyright holder does present such notices, the site operator will be held to a much tougher standard when evaluating actual knowledge of infringement. By the same token, if such notice is not utilized, it will be quite difficult, and

50. See *UMG Recordings*, 667 F.3d at 1037; see also 17 U.S.C. § 512(c)(1)(C) (2006).

51. *UMG Recordings*, 667 F.3d at 1036 (citing *Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1107 (W.D. Wash. 2004)); see also *Io Grp., Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132, 1148 (N.D. Cal. 2008) (same).

52. See Deborah A. Wilcox, *Resist Cease and Desist*, BUS. L. TODAY, May/June 2006, at 27, 31 (explaining merits of conciliatory approach as alternative to traditional cease and desist letters in trademark-infringement dispute situations).

perhaps impossible, for the copyright holder to satisfy the actual knowledge standard.

B. YouTube

The other major part of current OCILLA jurisprudence is the more famous *YouTube* case in which the United States District Court for the Southern District of New York and Second Circuit grappled with essentially the same fact pattern at issue in *UMG Recordings*, but emphasized other aspects.⁵³ The appellate court held that while the specific knowledge of infringement standard applied by the lower court was correct, in this particular case, the Southern District erroneously concluded that it was impossible for a reasonable jury to conclude that it had been satisfied.⁵⁴

Both the Southern District and Second Circuit determined without discussion that YouTube qualified as a service provider.⁵⁵ Interestingly, neither court cited the Ninth Circuit's analysis of the issue, leaving it the definitive, if muddled, word on the topic.⁵⁶ Hopefully, future cases will shed more light on this critical, but thus far largely ignored, part of the analysis in this area.⁵⁷

The outcome of this case was again driven by an examination of the "specific notice of infringement" requirement of the statute.⁵⁸ According to the Second Circuit, the district court took a broad view of it:

In a June 23, 2010 Opinion and Order . . . , the District Court held that the defendants were entitled to DMCA safe harbor protection primarily because they had insufficient notice of the particular infringements in suit. In construing the statutory safe harbor, the District Court concluded that the "actual knowledge" or "aware[ness] of facts or circumstances" that would disqualify an online service provider from safe harbor protection

53. *Viacom Int'l Inc. v. YouTube, Inc.*, 676 F.3d 19 (2d Cir. 2012), *aff'g in part, rev'g in part* 718 F. Supp. 2d 514 (S.D.N.Y. 2010). An indication of the significance of the case is found in the six pages of *amici* that participated in the case.

54. *See id.* at 26.

55. *See id.* at 29-39.

56. *See UMG Recordings*, 667 F.3d 1022. *See In re Aimster Copyright Litig.*, 252 F. Supp. 2d 634 (N.D. Ill. 2002), for an example of a case where the issue was more clear-cut.

57. The District Court for the Southern District of New York has applied the broad approach of the Second Circuit in the *YouTube* case with respect to the service provider definition and, more generally, in determining on a motion for summary judgment that the defendant was entitled to the benefits of the safe harbor. *Obodai v. Demand Media, Inc.*, No. 11 Civ. 2503 (PKC), 2012 WL 2189740, at *2-3 (S.D.N.Y. June 13, 2012). One wonders whether the precedential value of this case is impacted by the plaintiff proceeding pro se.

58. *See Viacom*, 676 F.3d at 30-32.

under § 512(c)(1)(A) refer to “knowledge of specific and identifiable infringements.”

The District Court further held that item-specific knowledge of infringing activity is required for a service provider to have the “right and ability to control” infringing activity under § 512(c)(1)(B). Finally, the District Court held that the replication, transmittal, and display of videos on YouTube constituted activity “by reason of the storage at the direction of a user” within the meaning of § 512(c)(1).⁵⁹

The Second Circuit made clear that the district court correctly held that actual knowledge of “specific instances of infringement” is required and relied heavily upon the *UMG Recordings* case in support, noting that it is the key element of the “limited body of case law” that is on point.⁶⁰ Its conclusion was:

Although the parties marshal a battery of other arguments on appeal, it is the text of the statute that compels our conclusion. In particular, we are persuaded that the basic operation of § 512(c) requires knowledge or awareness of specific infringing activity. . . . [T]he language of the statute . . . requires “expeditious[]” action to remove or disable “*the material*” at issue.

. . . .

Based on the text of § 512(c)(1)(A), as well as the limited case law on point, we affirm the District Court’s holding that actual knowledge or awareness of facts or circumstances that indicate specific and identifiable instances of infringement will disqualify a service provider from the safe harbor.⁶¹

Judge Cabranes emphasized that even a finding that over fifty percent of the postings on the site were infringing was, of itself, not sufficient to cause a finding adverse to the defendant on the notice issue.⁶²

However, in applying this standard, the Second Circuit provided some additional guidance. In particular, the court overturned the grant of summary judgment to defendants, reasoning that such a disposition would be premature.⁶³ Pointing to a number of internal YouTube e-mails discussing the status of specific copyrighted videos that appeared on the site, the court determined that this might have allowed a reasonable jury to find the requisite knowledge.⁶⁴ This seems logical in view of the detail

59. *See id.* at 26 (citations omitted).

60. *See id.* at 31-32.

61. *Id.* at 30-32 (quoting 17 U.S.C. § 512(c)(1)(A)(iii) (2006)) (second alteration in original).

62. *See id.* at 33.

63. *See id.* at 34.

64. *See id.* at 33-34.

contained in the e-mails and should give pause to those who conduct such a discussion in writing.⁶⁵

The court also took to task the district court for its application of the “no financial benefit” portion of the statute.⁶⁶ While the Second Circuit determined “that the ‘right and ability to control’ infringing activity under § 512(c)(1)(B) ‘requires something more than the ability to remove or block access to materials posted on a service provider’s website,’” it struggled with the question of what constituted “something more.”⁶⁷

Citing the only case to hold that a service provider could rightfully control infringing activity per §512(c)(1)(B), the Second Circuit encouraged the district court on remand to use the factors utilized by this lower court as guidance for determining whether YouTube had the right and ability to control the infringing activity. Under the lower court’s ruling, control exists “where the service provider instituted a monitoring program by which user Web sites received ‘detailed instructions regard[ing] issues of layout, appearance, and content.’ The service provider also forbade certain types of content and refused access to users who failed to comply with its instructions.”⁶⁸ The Second Circuit ordered the district court to consider whether YouTube’s operation of its site and related policies satisfied this standard, thereby causing YouTube to be deemed to have the requisite financial interest to nullify the availability of the safe harbor.⁶⁹ While the message of this action is not altogether clear, it does suggest that operators of sites allowing public submissions

65. For example:

[I]n an August 9, 2005 e-mail exchange, Hurley [a YouTube founder] urged his colleagues “to start being *diligent* about rejecting copyrighted/inappropriate content,” noting that “there is a cnn clip of the shuttle clip on the site today, if the boys from Turner would come to the site, they might be pissed?” Again, Chen [another founder] resisted . . .

Id. at 34. Despite its legal conclusion, the district court stated that a jury could find the defendant “welcomed” the posting of infringing material. *Id.* at 29 (quoting 718 F. Supp. 2d 514, 518 (S.D.N.Y. 2010)). The Second Circuit also made clear in a footnote that even the e-mails that were cited were not necessarily sufficient for the plaintiffs to make a prima facie case let alone prevail at trial: “We express no opinion as to whether the evidence discussed above will prove sufficient to withstand a renewed motion for summary judgment by YouTube on remand.” *Id.* at 34 n.9.

66. *See id.* at 36-38 (citing 17 U.S.C. § 512(c)(1)(B) (“[A]n eligible service provider must 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.” (internal quotation marks omitted))).

67. *Id.* at 38 (citations omitted).

68. *Id.* (quoting Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1173 (C.D. Cal. 2002) (citations omitted)).

69. *See id.*

should be as generic as possible in enumerating what they will and will not accept.

Finally, the court also considered whether the threshold “by reason of” language, which serves as a condition precedent to the availability of the statute, had been satisfied here. It determined that the performance of some preparatory work for videos before they are posted did not negate the safe harbor, which is seen as extending to “more than mere electronic storage lockers.”⁷⁰ However, while the court recognized that safe harbor beneficiaries must do something with submitted videos other than simply pass them through to their Web site and that various technical steps must be performed in order to make them practically accessible, the court balked at allowing all postdisplay steps.⁷¹

Specifically, the court found that YouTube made certain manually selected videos on its site available (through so-called “syndication” or licensing) to particular third parties, such as Verizon Wireless, even going so far as to “transcode” the videos to facilitate their use.⁷² The court felt that this level of involvement with the content may be sufficient to negate the “by reason of” condition precedent and asked the district court to conduct further proceedings directed to this issue.⁷³ However, because it was unclear whether any of the syndicated videos were the ones for which the plaintiffs’ copyrights had actually been infringed, it directed that the further proceedings address this issue as well.⁷⁴

C. Grokster

While it is not in itself a DMCA case, the U.S. Supreme Court’s action in *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.* involving copyright infringement resulting from so-called peer-to-peer file sharing is also highly pertinent to this discussion.⁷⁵ It involved the efforts of major media copyright holders, such as the plaintiffs in *UMG Recordings* and *YouTube*, to sue a firm that created and circulated file-copying software for undisputed infringement of their copyrights by various third parties.⁷⁶ This effectively cheated the copyright holders out

70. *Id.* at 38-40 (relying upon the determination of the District Court for the Central District of California in *UMG Recordings, Inc. v. Veoh Networks, Inc.*, 620 F. Supp. 2d 1081, 1088 (C.D. Cal. 2008)).

71. *See id.* at 38-39.

72. *See id.* at 40.

73. *See id.* at 42.

74. *See id.*

75. *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005).

76. *See id.* at 920-21.

of the fee they would have earned from a purchase by the person doing the copying.

The Court rejected the defendant's argument that it had not infringed on plaintiff's copyright, holding, "[O]ne who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties."⁷⁷ The Court relied on the Sony Betamax case to differentiate devices that have material noninfringing uses from those that do not.⁷⁸

There was no question about the defendant being a service provider, so the safe harbor was not invoked. However, the Court's focus on the defendant's intent⁷⁹ is a pertinent backdrop to DMCA analysis, where the issue is also the liability of a third party for someone's infringement. In fact, in its YouTube opinion, the Second Circuit briefly referenced the Supreme Court's guidance, when it discussed YouTube's financial interest in the infringing activity, citing *Grokster* as sufficiently analogous supporting authority, regardless of the difference in proposition: "The common law imposes liability for vicarious copyright infringement '[w]hen the right and ability to supervise coalesce with an obvious and direct financial interest in the exploitation of copyrighted materials—even in the absence of actual knowledge that the copyright mono[poly] is being impaired.'"⁸⁰

Commentators argue, with great plausibility, that cases such as *Grokster* are the foundation for today's thriving legal music download business—e.g., iTunes and its progeny.⁸¹ As a result, they must be taken

77. *Id.* at 936-37.

78. *See id.* at 933 (citing *Sony Corp. v. Universal City Studios*, 464 U.S. 417 (1984)). *Sony* barred secondary liability based on presuming or imputing intent to cause infringement solely from the design or distribution of a product capable of substantial lawful use, which the distributor knows is in fact used for infringement.

....

Sony's rule limits imputing culpable intent as a matter of law from the characteristics or uses of a distributed product.

Id. at 933-34.

79. The defendant's intent was very clearly established from a number of e-mails indicating the desire to become embroiled in litigation as a promotional technique. *See id.* at 924. In view of the defendants' brazen infringements, one wonders what to take from this case; given the textbook examples of wrongful intent, any other result would have been quite surprising.

80. *Viacom Int'l Inc. v. YouTube, Inc.*, 676 F.3d 19, 36 (2d Cir. 2012) (alterations in original) (quoting *Metro Goldwyn-Mayer*, 545 U.S. at 930 n.9).

81. *E.g.*, Kevin Werbach, *Digital Content: The Half-Full Glass*, WHARTON MAG., Spring 2012, at 20, available at <http://whartonmagazine.com/issues/spring-2012-2/digital-content-the-half-full-glass/> ("Napster [(a predecessor of Grokster that Grokster management sought to

into account when determining the implications of cases that are expressly devoted to the DMCA.

VI. CASE LAW OVERVIEW

What lessons should we learn about the OCILLA safe harbor from these cases? The short answer could be “none, for those outside the Second and Ninth Circuits” because they are the only ones to consider these issues to any significant degree. However, this would be a mistake in view of the facts that these circuits are quite influential to other circuits and that for the foreseeable future,⁸² their pronouncements are the most authoritative guidance available. The cases support a broad construction of the service provider definition, at least subject to anyone taking up Judge Fisher on his footnote observation as to the failure of the *UMG Recordings* plaintiff to contest the issue.⁸³ Both cases make clear that mere general knowledge by the operator of the existence on a site of infringing posts does not negate the availability of the safe harbor.

The Ninth Circuit appears more willing to accept compliance with defendants’ procedural obligations as at least a prima facie demonstration of the absence of knowledge of specific infringements, while the Second Circuit’s insistence upon allowing a jury determination of the matter based primarily upon the defendants’ syndication of some of the content suggests a greater skepticism. It appears that in both courts, procedural compliance for both plaintiffs and defendants is paramount: plaintiffs must provide statutory takedown notices before being able to recover, and defendants must promptly respond to such notices. It is fair to say, as the Second Circuit admits, that there is in some sense a bias in favor of service providers when construing this statute: “The Court of Appeals ‘reach[ed] the same conclusion’ with respect to the red flag provision, noting that ‘[w]e do not place the burden of determining whether [materials] are actually illegal on a service provider.’”⁸⁴

emulate)] and its ilk were sued out of existence. The promised market for licensed music developed. Apple parlayed iTunes into a multibillion-dollar business.”)

82. “[M]any courts look to the Second Circuit for guidance in copyright matters” Kramarsky, *supra* note 8. Even if the U.S. Supreme Court is willing to take up the *YouTube* case, which is questionable in itself, it seems doubtful, and perhaps impossible, that it could do so until after the case is revisited by the district court.

83. *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 667 F.3d 1022, 1030 n.4 (9th Cir. 2011).

84. *Viacom*, 676 F.3d at 32 (alterations in original) (quoting *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1114 (9th Cir. 2007)).

VII. APPLICATION OF THE CASE LAW

While existing OCILLA jurisprudence is sparse and far from definitive guidance to participants in the electronic media field, and the legislative history does relatively little to augment our understanding of rights and obligations, there are still several valuable takeaways from these cases which should guide practice and analysis in this arena.

For example, few would argue with the advisability for site operators to post on the site in “Terms of Use” or similar sections self-serving but unequivocal admonitions not to submit unlicensed copyrighted material. It is probably unrealistic to expect the average site user (or perhaps even attorneys versed in copyright law) to understand, let alone comply with, such terms, but their absence would appear to speak volumes. Indeed, the Ninth Circuit attributed great significance of “Terms of Use” in *UMG Recordings*.⁸⁵ In particular, Judge Fisher referred to Publisher Terms and Conditions (PTC) that provide:

[U]sers . . . “may not submit [material] . . . that contains any . . . infringing . . . or illegal content” and directs that they “may only upload and publish [material] on the Veoh Service to which [they] have sufficient rights and licenses to permit the distribution of [their] [material] via the Veoh Services.” The PTC agreement also gives Veoh a license to “publicly display, publicly perform, transmit, distribute, copy, store, reproduce and/or provide” the uploaded video “through the Veoh Service, either in its original form, copy or in the form of an encoded work.”

. . . The Terms of Use provide that “you expressly represent and warrant that you own or have the necessary licenses, rights, consents, and permissions to use and authorize Veoh to use all . . . copyright or other proprietary rights in and to any and all [material shared on Veoh].”⁸⁶

Other language that was mentioned approvingly, and worthy of note both for its substance and presentation, apart from copyright considerations,⁸⁷ was, “Do not upload videos that infringe copyright, are pornographic, obscene, violent, or any other videos that violate Veoh’s Terms of Use.”⁸⁸

Whether in view of other activities in which the *UMG Recordings* approach differed from the *YouTube* approach, or simply a difference in perspective between the Second and Ninth Circuits, similar terms were not viewed as favorably by the Second Circuit:

85. See *UMG Recordings*, 667 F.3d at 1027.

86. *Id.* (alterations in original).

87. It will be of little consolation for someone to be absolved of copyright infringement, but found liable for libel or distribution of prohibited obscene material.

88. *UMG Recordings*, 667 F.3d at 1027. Note the discussion of the need for site operators to address exposure from obscene, defamatory, or violent material, *infra* Part VIII.

The registration process requires the user to accept YouTube's Terms of Use agreement, which provides, *inter alia*, that the user "will not submit material that is copyrighted . . . unless [he is] the owner of such rights or ha[s] permission from their rightful owner to post the material and to grant YouTube all of the license rights granted herein."⁸⁹

In addition to the aforementioned terms of service qualifiers, site operators should employ certain precautionary measures including:

- (1) Rigorous compliance with the letter of the procedural steps mandated for all under the statute, such as giving notice of infringement to the agent designated in the statute, as opposed to (or in addition to) providing such notice through other channels, and proper designation of such agent;⁹⁰ and
- (2) Prompt, nondiscriminatory compliance with takedown notices and repeat offender policies.⁹¹ While this may not ultimately be sufficient to perfect a safe harbor defense to infringement claims when some copyrighted material does remain on the site for a substantial period, it was a significant influence on the district court's grant of summary judgment to defendants in *YouTube*, and is likely to be similarly relevant to other courts, and may even dissuade some copyright holders from bringing suit in the first place.⁹²

The significance of procedural compliance was underscored by the District Court for the Southern District of New York in a very recent case applying *YouTube*.⁹³ The court emphasized that the defendant had properly designated a copyright agent, promulgated appropriate terms of service, and complied with takedown notices.⁹⁴ Absent contrary decisions in other circuits and/or clarifying legislation, one can expect other lower courts, at least within the Second Circuit, to use a similarly mechanistic approach.

89. *Viacom*, 676 F.3d at 28. Notwithstanding the remand of the case for reconsideration of the summary judgment granted to the defendant, it still appears that this defendant would have fared worse in both the trial and appellate courts, absent such requirement.

90. 17 U.S.C. § 512(c)(1)(C), (2) (2006). While it is not clear whether it was determinative, in *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, Judge Fisher specifically noted that the plaintiff did not provide any takedown notice to the defendant, but that the only notice of infringement was sent by the Recording Industry Association of America. *See* 667 F.3d 1022, 1028 (9th Cir. 2011).

91. 17 U.S.C. § 512(c)(1)(C), (i)(1)(A).

92. *See Viacom Int'l Inc. v. YouTube, Inc.*, 718 F. Supp. 2d 514 (S.D.N.Y. 2010).

93. *Obodai v. Demand Media, Inc.*, No. 11 Civ. 2503 (PKC), 2012 WL 2189740 (S.D.N.Y. June 13, 2012).

94. *See id.* at *8-9.

VIII. SITE MONITORING? BANE OR BOON, AND FOR WHOM?

A step which is not clearly defined but worthy of consideration by practitioners, commentators, and the bench is the monitoring of sites for infringing material. It is true that the statute expressly provides that such action is not required to perfect a safe harbor defense.⁹⁵ It is also true that the Second Circuit's analysis in *YouTube* suggests that where a site operator makes decisions as to what to do with particular video clips that are not prompted by takedown notices, it risks running afoul of the condition precedent to the availability of the defense.⁹⁶

However, there are three reasons why such action may be advisable. First, site monitoring is not prohibited by any statute. Second, apart from copyright considerations, monitoring may be advisable to avoid liability for the posting of defamatory, obscene, or violent material.⁹⁷ Suggesting that monitoring be confined only to such issues and overlook material that is palpably infringing, such as a movie clip, seems unrealistic.

Although there is no written legal analysis as of yet, this conundrum has been discussed informally, albeit graphically, at the *Wall Street Journal's* 2012 "All Things Digital" conference. Ari Emanuel, a recognized agent for many high-profile entertainers featured in copyrighted content, angrily lamented the ability of intermediaries such as Google to filter out child pornography while claiming to be unable to stop infringement: "They decide when they want to police stuff and when they don't. Child pornography—they can actually filter that. They stop those people."⁹⁸ In response, Google executive Susan Wojicki observed: "The problem is that identifying which copyright belongs to whom is very complicated. It's not like child porn."⁹⁹ Mr. Emanuel has the better argument. If material is clearly infringing, it should be removed, irrespective of whether its rightful owner can be readily identified. It does seem disingenuous for an intermediary to claim it can only identify one type of inappropriate content. Perhaps the difficulty identifying the owner makes it problematic to perfectly screen infringing

95. 17 U.S.C. § 512(m)(1).

96. 676 F.3d 19, 41 (2d Cir. 2012).

97. The defendant in *UMG Recordings* does perform such manual monitoring for pornography, a fact not preventing summary judgment in its favor. 667 F.3d 1022, 1027 n.2 (9th Cir. 2011).

98. *Stop, Thief!*, WALL ST. J. (June 4, 2012), <http://online.wsj.com/article/SB10001424052702303640104577442390564645770.html>.

99. Walt Mossberg, *The Problem with Copyrights*, WALL ST. J. (June 4, 2012), <http://online.wsj.com/article/SB10001424052702303640104577440992894308240.html>. This article also notes Ms. Wojicki's point that Google has spent a good deal of money on a system called "Content ID" which is intended to filter out copyrighted material.

posts, but this does not mean that the effort is useless. One would anticipate this enigma being increasingly relevant in legal proceedings.

Finally, whatever may be the disposition of this issue in a court case, some level of monitoring may allow these cases to be avoided in the first place. While some copyright holders may sue as a result of the appearance of their material on a Web site, notwithstanding its prompt takedown upon their request, others may be mollified if they see the site operator making good faith efforts to screen out their material without prompting. Even assuming *arguendo* that monitoring will increase an operator's legal exposure by prompting the finding of control of site content, this is beside the point if such monitoring obviates the need to bring the case. The trade-off between these considerations is well worth discussion "on the ground" by those operating sites and those advising them and would be a useful topic for future commentary.

IX. A TECHNOLOGICAL ALTERNATIVE

One step, which is perhaps harder to understand, is the use of so-called "digital fingerprints" or "watermarks" to identify and screen for copyrighted material. Judicious use of this technique may serve as a fair accommodation of the rights of all participants in this space. Without converting this Article into an engineering treatise, let it suffice to say that this technique involves using computer code to "mark" copyrighted content in a distinguishing manner, so that it may be recognized by a scanning device that has been updated with information.¹⁰⁰ The scanning device can then prompt human analysts to consider appropriate action such as determining whether the material at issue is actually copyrighted and taking it down—or not posting it at all—if they have reason for concern. While this technique is far from perfect and often produces "false positives," it is in commercial use today.

It has, however, been tacitly endorsed by the Ninth Circuit in *UMG Recordings*.¹⁰¹ Judge Fisher's opinion in favor of the defendants referred to the use of multiple technologies to screen out copyrighted material and in particular emphasized the "digital fingerprints":

100. At the Web site HowStuffWorks, there is a fairly succinct discussion of this technique, the current extent of its use, and the manner in which it can be used to fairly protect the owners of digital content. It also distinguishes the use of this technology from its use to identify and track individual computer and internet users, which is far more controversial as a result of its impact on user privacy. Wesley Fenlon, *How Digital Fingerprinting Works*, HOWSTUFFWORKS, <http://computer.howstuffworks.com/digital-fingerprinting2> (last visited Oct. 12, 2012).

101. See *YouTube Birdsong Goof Shows Copyright Problems*, *supra* note 32, for discussion of such technology causing a birdsong video to be considered infringing.

Veoh employs various technologies to automatically prevent copyright infringement on its system. In 2006, Veoh adopted “hash filtering” software. Whenever Veoh disables access to an infringing video, the hash filter also automatically disables access to any identical videos and blocks any subsequently submitted duplicates. Veoh also began developing an additional filtering method of its own, but in 2007 opted instead to adopt a third-party filtering solution produced by a company called Audible Magic. Audible Magic’s technology takes audio “fingerprints” from video files and compares them to a database of copyrighted content provided by copyright holders. If a user attempts to upload a video that matches a fingerprint from Audible Magic’s database of forbidden material, the video never becomes available for viewing. Approximately nine months after beginning to apply the Audible Magic filter to all newly uploaded videos, Veoh applied the filter to its backlog of previously uploaded videos. This resulted in the removal of more than 60,000 videos, including some incorporating UMG’s works.¹⁰²

While the court did not expressly state that use of this technique dictated the outcome, its extensive discussion implies that it was influential, as an indication of defendants’ in good faith, and a genuine exclusion of a great deal of copyrighted material. This technique was not discussed in the *YouTube* case. It is unclear if this is because it was not utilized (although it is apparently utilized today through a system known as “Content ID”) or if the court would have attributed little legal significance to it even if it had been.¹⁰³

Given the unsettled state of the law in this area, it is logical for other courts to follow suit, because this step requires no grappling with the nuances of statutory construction or technical mechanisms. Use of this technique in some form reasonably reflecting then commercially available technology is an important step in the development of law and practice in this area. As noted by Judge Cabranes, a separate provision of the DMCA, 17 U.S.C § 512(i), addresses the topic in very general terms.¹⁰⁴ However, it does not have any clear connection to the safe harbor in subsection (c) and does not apply at all to copyright owners: “In addition, a qualifying service provider must accommodate ‘standard technical measures’ that are ‘used by copyright owners to identify or protect copyrighted works.’”¹⁰⁵ Judge Cabranes suggests that if such

102. *UMG Recordings*, 667 F.3d at 1028.

103. *See YouTube Birdsong Goof Shows Copyright Problems*, *supra* note 32.

104. *Viacom Int’l Inc. v. YouTube, Inc.*, 676 F.3d 19, 27 (9th Cir. 2012).

105. *Id.* (citing 17 U.S.C. §§ 512(i)(1)(B), (i)(2) (2006)).

fingerprinting is considered a “standard technical measure,” failure to use it may negate the availability of the safe harbor.¹⁰⁶

It would behoove Congress to address this ambiguity by adding language to this effect to the OCILLA statute. For example, it might enact a new subsection stating:

In any legal action in which a party claims the benefits of this subsection (c), the court is directed to take into account (i) the extent to which such party has utilized then-commercially-available technology to identify and screen submitted content in order to exclude from its site unlicensed copyrighted material, and (ii) the extent to which any party claiming an infringement has utilized the technology referenced in (i) above to provide notice to others of the existence of its interest. The use of such technology shall not, of itself, be deemed to provide such party with control over such content within the meaning of any portion of this subsection (c).¹⁰⁷

Greater use of such a technique is likely to benefit all market participants. Site operators, Internet service providers, and Web hosting firms can use it to minimize (but not entirely eliminate) problems associated with infringing posts¹⁰⁸ without much regard for the subjective analysis discussed in this Article. To the extent infringing material is kept out, one need not consider whether they are a service provider, have “too much control” over content, should manually monitor the site for infringement, or have an excessive financial interest.

If the suggested statutory amendment is enacted, and firms use the technique, they should be able to operate their businesses with a reasonable expectation that their good faith will largely or entirely protect them in the rare instances where they are challenged for letting infringing material reach the public. By the same token, copyright holders would be the victims of far less infringement than at present and should be able to address infringement in more expedient fashion.¹⁰⁹ The service

106. *See id.* at 41. However, it is far from clear that this is consistent with the statutory scheme and what constitutes a “standard technical measure” today or in the future. “Refusing to accommodate or implement a ‘standard technical measure’ exposes a service provider to liability; refusing to provide access to mechanisms by which a service provider affirmatively monitors its own network has no such result.” *Id.*

107. If the cost of such technology is deemed prohibitive, a minimum size (such as revenue) could be included as a condition precedent.

108. Assuming that copyright holders use it as well.

109. *See* Vauhini Vara, *Photo Agencies Scour the Web for Copyright Violations*, WALL ST. J. (Oct. 14, 2005), http://online.wsj.com/public/article/SB112897424251164666-0mFu92_5xrCHDRrqLE9YeCOOnI_20061015.html?mod=tff_main_tff_top (discussing the use of this technology with both music and still pictures, and, more importantly in the opinion of the author, as a mechanism to facilitate the voluntary resolution of disputes by prompting parties to enter into license agreements).

provider's use or failure to use the technique should be a major and perhaps determinative factor, which should make for less litigation. Even if this is not the case, there should be much less need for the exhaustive discovery that is currently needed to establish facts like someone's level of knowledge, financial interest, and control over content.

Even without congressional action, it still makes sense for market participants, particularly the larger ones, to speed the implementation of this technology. Doing so is likely to minimize the need to deal with the arcane issues discussed in this Article, either by avoiding infringements or by providing to any court that does address them clear evidence of the pertinent party's good faith.

X. REVISITING WHO IS A SERVICE PROVIDER: AN INVITATION TO ARGUMENTATION AND LEGISLATION

An additional topic that warrants significant legislative and judicial attention and may be fertile ground for copyright holders to pursue in future litigation is the issue of who falls under the statute's "service provider" classification. As noted above,¹¹⁰ the limited consideration of this statute by the courts has involved little analysis of this term, leading to the presumption that seemingly anyone connected to the Internet qualifies. The author is not aware of any case in which anyone has been found not to be a service provider.

Based upon the language of the definition, this seems inappropriate.¹¹¹ Looking at the operative phrases, "an entity offering the transmission, routing, or providing of connections for digital online communications" and "a provider of online services or network access," it is hard to understand how they clearly cover Web site operators and even hosting companies.¹¹² One can easily see how this language is intended to immunize those who create and maintain the Web's "plumbing"—such as Internet service providers like AT&T, Comcast, and the like—from liability for offending transmissions by their users. Such firms certainly do offer transmission services and network access and have little or no practical ability to evaluate transmissions for compliance with law. Even granting the different purposes served by the two quoted branches of the statute, it is difficult to imagine how firms like YouTube or anyone else operating a Web site accepting public

110. *See supra* Part IV.A.

111. *See supra* Part IV.A.

112. *Id.*

submissions of creative materials such as music and movies are clearly and unequivocally covered.¹¹³

There appears to be no way to even argue that they provide transmission, routing, or connections for anything, particularly in a wireless access world. They also do not provide network access. One can perhaps plausibly argue that some such firms provide “online services” of some sort, especially in the absence of a definition or common meaning of the term. This may be true of the Amazons and eBays of the world, which do provide some sort of brokerage service with a charge to their users.¹¹⁴ It is much harder to ascertain what service is provided, and to whom, by sites such as YouTube that are sustained by advertising revenue and solicit creative submissions. This argument is not a legal “slam dunk” or a foregone conclusion.

Moreover, it is equally problematic to assert that all entities with Web sites allowing public submissions can come within the online service provider term. What service—online or otherwise—is provided by a company requesting that consumers submit videos describing their experiences with the company’s products? One could argue that the inclusion of copyrighted material in such a submission should not, as a matter of public policy, subject the site operator to infringement liability, but it is hard to see how this result is compelled, or even permitted, by the existing language of the statute.

As noted *supra*, it seems disingenuous to argue that Congress intended to validate business and technological practices that did not exist when it enacted the DMCA. Even giving credit for anticipation of rapid technological progress, it seems to be a stretch to conclude on the basis of legislative history and statutory language that Congress favored broad protection for services like Veoh and YouTube when nothing like them existed or would exist for several years after the enactment of the DMCA. Even digital music, which is at the heart of much of today’s controversy, was at a very early stage back then, and digital video did not exist.

It would be optimal if Congress could address this topic as well as the potential benefits from “digital fingerprinting.” As a matter of policy,

113. One branch applicable to 17 U.S.C. § 512(a) and the other, broader version applicable to § 512(c) would have to be distinguished in cases where the defendant appears to come within one and not the other, depending on which prong of the safe harbor was invoked.

114. *See, e.g., Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090 (W.D. Wash. 2004) (holding that Amazon meets the DMCA definition of service provider), *overruled on unrelated issue in Cosmetic Ideas, Inc. v. IAC/InteractiveCorp*, 606 F.3d 612 (2010); *Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082, 1087 (C.D. Cal. 2001) (holding that eBay “clearly” falls within the broad definition of a service provider).

one can certainly justify the current broad interpretation of the term. Both the congressional purpose of promotion of the growth of the Internet and the existing extensive reliance on the broad reading of the term support such action. However, in view of the numerous demands on Congress's time, one should not assume that this will be the case.

In the meantime, the author believes that the bench, particularly in circuits where there is no case on point, should be more rigorous in its analysis of this issue when asked to apply the safe harbor. While it is not altogether clear who has the burden of proof with respect to a service provider's status, because the safe harbor is an affirmative defense in accordance with customary litigation practice, one would expect the party invoking the defense to have this burden, or at least the burden of going forward with some rationale.¹¹⁵ Therefore, judges should not perfunctorily assume that this burden has been met and proceed to apply the rest of the provision, absent meaningful pleading and proof that the defendant is actually a service provider.

In addition, copyright holders who sue for infringement should contest the issue where appropriate. Unless the suit is brought against a traditional Internet service provider or very similar firm, they should also argue in support of the safe harbor that even if the defendant does establish the safe harbor's requisite lack of control and financial interest and has followed appropriate procedures (such as agent designation), it cannot qualify for this protection because it is not a service provider. Judge Fisher's express comment on the plaintiff's failure to make such an argument in *UMG Recordings* suggests that had they done so, there would have at least been a genuine issue to decide.¹¹⁶

While the *UMG Recordings* and *YouTube* cases can certainly be invoked for the proposition that virtually anyone with a Web presence is a service provider, their lack of analysis of the topic and the failure of the Second Circuit to cite the relative *UMG Recordings* discussion in *YouTube* reduces their persuasive value. In any event, this issue is a matter of first impression outside the Second, Seventh, and Ninth Circuits.

Given the critical nature of this term to the entire safe harbor, it is the author's hope that whatever is done by Congress, the bench, and

115. See Ronald J. Allen, *Presumptions, Inferences and Burden of Proof in Federal Civil Actions—An Anatomy of Unnecessary Ambiguity and a Proposal for Reform*, 76 NW. U. L. REV. 855, 892 (1982). (summarizing traditional federal practice regarding burdens of pleading and proof).

116. See *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 667 F.3d 1022 (9th Cir. 2011).

private litigants, other commentators will weigh in on the topic in order to provide guidance to market participants. The matter is too important to be left to the cursory references that have thus far been all we have. Even if we end up with the broad construction of the term favored in the Second and Ninth Circuits, we should get there through a much more principled process.

XI. CONCLUSION

Congress did the public a significant service by enacting the DMCA and OCILLA. Without these provisions, it is doubtful that we would have the robust Internet that is today such a key driver of our economy. Nevertheless, the current state of language and jurisprudence under OCILLA is so vague and, to some extent, misguided that it threatens to lead to anomalous results and, in any event, fails to provide the required guidance to market participants—both copyright holders and Web site operators—and their advisors to allow continued development of Internet-based commerce. Hopefully, this Article can at least prompt the sort of discussion, litigation, and basis for improvement in law and practice that are needed to facilitate fair and improved reconciliation of the interests of all market participants. Such improvement should be manifested in argumentation, adjudication, and technological innovation.